Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1240

(04/2008)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité du cyberespace – Lutte contre le pollupostage

Technologies intervenant dans la lutte contre le spam par courrier électronique

Recommandation UIT-T X.1240

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	**X.1230–X.1249**
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1240

Technologies intervenant dans la lutte contre le spam par courrier électronique

Résumé

La Recommandation UIT-T X.1240 spécifie les concepts fondamentaux, les caractéristiques et les effets du spam par courrier électronique ainsi que les technologies intervenant dans la lutte contre le spam par courrier électronique. Elle présente en outre les solutions techniques existantes et les activités connexes réalisées par diverses organisations de normalisation et par les organismes compétents de lutte contre le spam par courrier électronique. Elle contient des indications et des informations à l'intention des utilisateurs qui souhaitent développer des solutions techniques de lutte contre le spam par courrier électronique. Cette Recommandation servira de base à l'élaboration d'autres Recommandations techniques sur la lutte contre le spam par courrier électronique.

Source

La Recommandation UIT-T X.1240 a été approuvée le 18 avril 2008 par la Commission d'études 17 (2005-2008) de l'UIT-T selon la procédure définie dans la Résolution 1 de l'AMNT.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT [avait/n'avait pas] été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Introduction

Comme cela a été demandé dans la Résolution 52 de l'AMNT 04 ‘Lutte contre le pollupostage [spam] par des moyens techniques', des travaux de normalisation ont été entrepris pour élaborer des Recommandations UIT-T qui aident à lutter contre le spam par des moyens techniques. La présente Recommandation fait partie d'une série de Recommandations UIT-T sur la lutte contre le spam par courrier électronique, qui énoncent des lignes directrices, des spécifications, un cadre technique et des stratégies techniques. D'autres Recommandations UIT-T sur la lutte contre le spam dans les applications multimédias IP telles que la téléphonie IP, la messagerie instantanée et les conférences seront élaborées en tant que documents distincts.

Recommandation UIT-T X.1240

Technologies intervenant dans la lutte contre le spam par courrier électronique

1 Domaine d'application

La présente Recommandation spécifie les technologies intervenant dans la lutte contre le spam par courrier électronique, ou pourriel. Elle présente les solutions techniques existantes et les activités connexes réalisées par diverses organisations de normalisation et par les organismes compétents de lutte contre le spam par courrier électronique. Elle a pour objet de donner des informations utiles aux utilisateurs qui souhaitent développer des solutions techniques de lutte contre le spam par courrier électronique. La présente Recommandation servira de base à l'élaboration d'autres Recommandations techniques sur la lutte contre le spam par courrier électronique.

NOTE – L'utilisation du terme "identité" dans la présente Recommandation ne lui confère pas une valeur absolue, et ne constitue pas en particulier une validation positive.

2 Références

Aucune.

3 Définitions

La présente Recommandation définit les termes suivants:

3.1 **hameçonneur**: entité ou personne qui lance des attaques par hameçonnage.

3.2 **hameçonnage**: les attaques par hameçonnage recourent à l'ingénierie sociale et à des subterfuges techniques pour dérober des informations personnelles et financières. Les stratagèmes fondés sur l'ingénierie sociale consistent à envoyer des courriers électroniques d'apparence légitime, contenant des liens vers des sites web contrefaits conçus pour tromper les destinataires afin de leur soutirer des données sensibles (telles que numéro de carte de crédit, nom d'utilisateur de compte, mot de passe et numéro de sécurité sociale). Usurpant des noms de marque de banques, de cybercommerçants et de sociétés de cartes de crédit, les hameçonneurs parviennent souvent à convaincre les destinataires de répondre. Les stratagèmes techniques consistent à installer des logiciels criminels dans les ordinateurs personnels pour dérober directement des données sensibles. On utilise souvent des logiciels espions enregistreurs de frappe de type cheval de Troie à cette fin.

3.3 **spam**: le sens du mot "spam" dépend de la perception du respect de la vie privée et de ce que constitue le spam au niveau de chaque pays, du point de vue technologique, économique, social et pratique. En particulier, ce sens évolue et se diversifie au fur et à mesure du développement des technologies, donnant lieu à de nouvelles possibilités d'utilisation abusive des communications électroniques. Bien qu'aucune définition du spam n'ait été adoptée à l'échelle mondiale, ce terme est couramment employé pour décrire des communications électroniques de masse non sollicitées transmises par courrier électronique (courriel) ou par messagerie mobile pour promouvoir des produits ou services commerciaux.

3.4 **spammeur**: entité ou personne qui crée et envoie des spams.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

API interface de programmation d'application (*application programming interface*)

CSV validation de serveur certifiée (*certified server validation*)

DKIM courrier identifié par clés de domaine (*domainkeys identified mail*)

DNS système de noms de domaine (*domain name system*)

DSN notification de statut de distribution (*delivery status notification*)

HTML langage de balisage hypertexte (*hypertext markup language*)

IM messagerie instantanée (*instant messaging*)

ISP fournisseur de services Internet (*internet service provider*)

META améliorations de message pour autorisation de transmission (*message enhancements for transmission authorization*)

MMS service de messagerie multimédia (*multimedia messaging service*)

MTA agent de transfert de courrier (*mail transfer agent*)

OCDE Organisation de coopération et de développement économiques

OPES services périphériques connectables ouverts (*open pluggable edge services*)

PGP confidentialité plutôt bonne (*pretty good privacy*)

PTR enregistrement de pointeur (*pointer record*)

SMS service de messages courts (*short message service*)

SMTP protocole simple de transfert de courrier (*simple mail transfer protocol*)

SPF cadre politique de l'expéditeur (*sender policy framework*)

TEOS norme ouverte sur le courrier électronique fiable (*trusted email open standard*)

5 Conventions

Aucune.

6 Introduction à la lutte contre le spam par courrier électronique

6.1 Concept et caractéristiques du spam

Bien qu'aucune définition du spam n'ait été adoptée à l'échelle mondiale, ce terme est couramment employé pour décrire des communications électroniques non sollicitées transmises par courrier électronique, par messagerie mobile (SMS, MMS) ou par messagerie instantanée, l'objectif étant généralement de promouvoir des produits ou services commerciaux.

Le spam par courrier électronique est le type de spam le plus répandu, mais le spam peut s'attaquer à d'autres cibles, par exemple la messagerie de téléphone mobile, la téléphonie IP, la messagerie instantanée, les forums de discussion de Usenet, les moteurs de recherche sur le web et les blogs. Le spam peut contenir aussi bien des publicités pour des biens que des photos pornographiques offensantes. Le spam par courrier électronique présente divers effets négatifs pour les utilisateurs de messagerie électronique et pour les fournisseurs de services Internet (ISP):

– Les destinataires de spams et les ISP dépensent beaucoup de temps, d'argent et d'efforts pour identifier, supprimer et filtrer les spams.

– Le spam par courrier électronique peut inclure un contenu trompeur pour attirer les destinataires de spam ou un contenu pour adultes inapproprié pour les enfants.

– Les utilisateurs de messagerie électronique et les ISP sont victimes du gaspillage de mémoire et de ressources de réseau.

– La propagation des virus et des logiciels espions peut constituer une menace pour la sécurité des réseaux.

– Le spam par courrier électronique réduit la visibilité des courriers électroniques normaux et importants.

Un phénomène récent et qui prend de l'ampleur consiste à utiliser des spams pour réaliser des activités frauduleuses et criminelles – y compris des tentatives de saisie d'informations financières (par exemple des numéros de compte et des mots de passe) en envoyant des messages déguisés semblant provenir de sociétés de confiance ("usurpation de marque" ou "hameçonnage") – ou à s'en servir de véhicule pour propager des virus et des vers.

Les attaques par hameçonnage recourent à l'ingénierie sociale et à des subterfuges techniques pour dérober des informations personnelles et financières. Les stratagèmes fondés sur l'ingénierie sociale consistent à envoyer des courriers électroniques d'apparence légitime, contenant des liens vers des sites web contrefaits conçus pour tromper les destinataires afin de leur soutirer des données sensibles (telles que numéro de carte de crédit, nom d'utilisateur de compte, mot de passe et numéro de sécurité sociale). Usurpant des noms de marque de banques, de cybercommerçants et de sociétés de cartes de crédit, les hameçonneurs parviennent souvent à convaincre les destinataires de répondre. Les stratagèmes techniques consistent à installer des logiciels criminels dans les ordinateurs personnels pour dérober directement des données sensibles. On utilise souvent des logiciels espions enregistreurs de frappe de type cheval de Troie à cette fin. Les logiciels criminels de détournement de domaine redirigent les utilisateurs vers des serveurs proxy ou des sites frauduleux, généralement par détournement ou empoisonnement de système de noms de domaine (DNS).

Les spammeurs font preuve d'une grande créativité pour éviter d'être détectés, par exemple en falsifiant l'origine des courriers électroniques et en rendant aléatoire leur contenu pour contourner les filtres antispams. L'ampleur du problème est devenue telle que des lois antispams sont rapidement promulguées dans un certain nombre de pays – même si les méthodes et solutions utilisées varient d'un pays à l'autre. Dans le même temps, il est de plus en plus admis que la lutte contre le spam est un problème qui exige une coordination et une coopération internationales.

6.2 Méthodes de lutte contre le spam par courrier électronique

Etant donné que le spam par courrier électronique cause des dommages considérables aux utilisateurs de messagerie électronique, aux ISP et aux opérateurs de réseau, des technologies ont été développées et des réglementations ont été adoptées dans un grand nombre de pays pour faciliter la lutte contre ce fléau. Toutefois, la lutte contre le spam n'étant pas un problème simple, il est difficile de mener efficacement cette lutte au moyen d'une seule mesure telle qu'un filtrage ou une sanction judiciaire; il convient donc d'appliquer simultanément diverses méthodes:

– Réglementation: il convient d'adopter des réglementations antispams pour faciliter une réaction appropriée des utilisateurs face aux spams par courrier électronique et pour renforcer l'effet des technologies antispams telles que le filtrage. De plus, une réglementation peut faciliter la protection des utilisateurs et des ISP contre les spams illégaux.

– Technologie: il est essentiel de développer des technologies antispams pour lutter efficacement contre de grandes quantités de spams par courrier électronique. Il est nécessaire de développer diverses technologies pour empêcher l'envoi de spams ainsi que pour identifier et filtrer efficacement les spams.

– Mesures prises par le secteur privé: il est utile que les acteurs du secteur privé tels que les ISP ou les opérateurs de réseau développent et installent divers types de technologies antispams, notamment des listes noires, des listes blanches et des fonctions de filtrage. Par ailleurs, les ISP peuvent adopter des principes de lutte contre le spam par courrier électronique.

– Coopération internationale: la coopération internationale est nécessaire, étant donné que les réseaux de télécommunication ne connaissent pas de frontières et que la production et

l'effet des spams dépassent les frontières nationales. La coopération internationale est également utile pour le partage d'informations sur l'adoption d'une réglementation efficace, le développement de technologies antispams et la sensibilisation des utilisateurs et fournisseurs de services.

– Sensibilisation: pour réduire au minimum les dommages causés par le spam par courrier électronique, il est important de sensibiliser les utilisateurs et les ISP. Cette sensibilisation devrait permettre aux utilisateurs de messagerie électronique de prendre des mesures appropriées concernant le spam par messagerie électronique et aux ISP d'adopter des principes et des technologies antispams.

Parmi les diverses mesures antispams présentées ci-dessus, la présente Recommandation se limite aux moyens techniques de lutte contre le spam et porte plus précisément sur le développement et l'application de technologies antispams.

7 Technologies antispams

Le rapport du groupe de réflexion sur le spam de l'OCDE [b-OECD TF] comprend plusieurs éléments sur la lutte contre le spam par courrier électronique, qui couvrent notamment les approches réglementaires, les problèmes de répression du spam et les solutions techniques. Ce paragraphe de la présente Recommandation s'appuie sur une partie de ce Rapport (Elément IV – Technologies antispams). L'attention du lecteur est attirée sur le fait que la boîte à outils antispams a été publiée en mai 2006 et qu'elle n'a pas été mise à jour depuis.

Ce paragraphe porte sur les différentes technologies antispams et les fonctions qu'elles peuvent proposer, ainsi que les méthodes qu'il faut appliquer lorsque l'on reçoit du spam. Le meilleur moyen de combattre efficacement le spam est d'utiliser avec discernement une combinaison de plusieurs technologies. Utilisée isolément, aucune des méthodes décrites ne donnera entièrement satisfaction. Lorsque plusieurs technologies antispams sont mises en place et fonctionnent en collaboration, cela peut diminuer considérablement le volume de spam qui affecte un système.

7.1 Introduction

Le spam pose des difficultés techniques complexes et les solutions mises en œuvre pour en venir à bout doivent s'appuyer sur des mesures techniques appropriées. Si l'intervention de la puissance publique et le rôle de la législation sont utiles, ils ne suffisent pas à répondre aux défis lancés par le spam. En effet, le spam est avant tout un problème technique qui résulte d'une faille dans le protocole SMTP. Du fait de la nature technique du problème, il est particulièrement difficile pour les autorités d'exécution d'identifier les spammeurs et donc de les sanctionner.

Bien qu'il existe diverses définitions du spam, des technologies et des techniques peuvent être mises en œuvre pour limiter le phénomène des courriels inopportuns. L'objet de ce paragraphe est de faire un tour d'horizon neutre des différents types d'outils et de méthodes de lutte, ainsi que des éléments à prendre en considération avant de mettre en œuvre ces parades. Nous faisons spécifiquement référence à des outils plutôt qu'à des solutions. La technologie est conçue pour répondre à une grande partie des problèmes posés par le spam, et elle pourrait effectivement "résoudre" une partie des problèmes spécifiques liés au spam, mais une solution globale au spam ne peut être atteinte qu'à travers une approche multifacettes à base de technologies, de mesures publiques (notamment de réglementation s'il y a lieu), de pratiques et de sensibilisation.

Les outils antispams interviennent à des niveaux multiples – au niveau du point d'origine, de la dorsale, du point d'entrée et dans la machine du destinataire – et peuvent être utilisés seuls ou en combinaison. On trouvera des informations actualisées et des ressources sur le site web de la boîte à outils à l'adresse www.oecd-antispam.org.

Ce paragraphe s'adresse en particulier aux gestionnaires de serveurs de messagerie et fait le point sur les forces et les faiblesses de chaque technique de filtrage afin de les aider à choisir leur solution

logicielle en fonction de leurs impératifs et de leurs besoins en matière de messagerie électronique et de l'architecture qu'ils prévoient. L'accent est mis ici sur les pratiques applicables au courrier entrant, même si celles destinées à réduire le spam sortant seraient également utiles. Les opérateurs des serveurs de réception ne sont pas les seuls à avoir un rôle à jouer. Les opérateurs des serveurs d'expédition peuvent recourir à une limitation du débit sortant et à un blocage du port 25 et employer d'autres mesures pour réduire le volume de spam envoyé depuis leurs serveurs.

Les outils antispams doivent intervenir à la fois sur le courrier et sur le comportement des utilisateurs en matière de messagerie. Etant donné cette multiplicité de facteurs, de nombreux instruments et méthodes s'appuient sur des séries de règles ou d'hypothèses opérant séparément ou en combinaison afin d'identifier les messages électroniques suspects. Peu à peu, le spam a envahi de nouveaux espaces et il véhicule toujours plus de virus et de logiciels malveillants. Cela nécessite une technologie défensive qui ne se limite plus aux outils de type textuel mais fait appel à des outils qui analysent des facteurs comportementaux et contextuels pour déterminer s'il convient d'accepter ou de rejeter tel ou tel courrier ou même certaines tentatives de connexion. Compte tenu de la menace accrue que le spam représente pour la sécurité, nous pensons que les technologies antispams s'appuieront davantage sur des technologies avancées de sécurité et d'authentification ou qu'elles devront être conjuguées à ce type de technologies.

7.2 L'importance de l'outil et du contexte technologique

Une partie des outils et des technologies examinés dans ce paragraphe sont spécifiquement conçus pour être mis en œuvre au point d'entrée de la plate-forme de messagerie électronique; d'autres peuvent être plus utilement déployés après la réception des messages mais avant leur présentation au destinataire final. Il est important de noter que certains outils résident également dans l'ordinateur du destinataire. A chaque niveau d'application du filtre, l'objectif d'une règle peut être soit de refuser ou de rejeter le message électronique, soit de le marquer, soit de le placer dans la boîte de spam de l'utilisateur final.

L'opportunité et l'utilité de chaque règle ne peuvent donc être estimées qu'en fonction du contexte précis dans lequel elle est appliquée, du niveau auquel elle est appliquée dans le processus de distribution des messages, et de ce qu'il advient de la communication en bout de course.

7.3 Combinaison de tests

La technologie doit être à la base de toute stratégie visant à venir à bout du spam. Il faut savoir qu'aucune des technologies examinées dans les paragraphes qui suivent ne constitue un remède miracle ou une solution universelle à tous les problèmes posés par le spam. Toutes les technologies sont complémentaires et leur efficacité sera optimale si elles sont employées en conjonction les unes avec les autres. L'intégration d'un certain nombre de technologies est nécessaire pour réduire l'impact négatif du spam sur un système.

Ces tests ne doivent pas nécessairement être utilisés en mode "tout ou rien". Il est préférable de les combiner afin de maximiser le nombre de messages de spam interceptés, tout en minimisant le nombre de courriels légitimes interceptés ou refusés à tort.

– Refus "tout ou rien": c'est l'une des actions possibles pour les services qui utilisent une liste noire. Tout message qui ne passe pas le test est refusé. L'occurrence d'erreurs dépend toutefois du point où est appliquée la règle dans le processus de distribution.
– Privilège d'accès: c'est l'une des actions possibles pour les serveurs qui utilisent une liste blanche. Tout message qui passe le test est accepté. Pas de risque de rejet de messages légitimes, mais risque de faux négatifs. Par exemple, une liste blanche de domaines n'a pas vraiment d'intérêt si le domaine de l'expéditeur n'est pas authentifié (avec SPF ou DKIM).
– De nombreux messages de spam ou vers se revendiquent de marques reconnues dans l'espoir de bénéficier de privilèges d'accès.

– Notation: c'est de cette façon que des programmes combinent plusieurs tests. La notation est vivement recommandée pour éviter les inconvénients du "tout ou rien" mais elle est coûteuse en ressources machines et demande une mise à jour permanente des facteurs de notation afin d'optimiser la détection tout en minimisant les faux positifs.

La méthode classique est d'appliquer plusieurs tests "tout ou rien", puis d'attribuer une notation aux messages qui ont été autorisés.

7.4 Types de technologies antispams

7.4.1 Authentification du courrier électronique

Les méthodes d'authentification du courrier relèvent de la catégorie des règles qui, si elles contribuent à la lutte contre le spam, ne constituent pas des technologies spécifiques antispams.

Cet aspect est plus facile à comprendre si on a recours à une analogie. Une carte d'identité ne constitue pas une marque de confiance, dans la mesure où les malfaiteurs peuvent aussi en avoir une. Mais l'obligation de la transparence est plus favorable aux expéditeurs légitimes qu'aux spammeurs.

7.4.2 SPF ou Sender-ID

L'un des principaux facteurs qui favorisent la prolifération du spam est la possibilité pour les spammeurs de masquer la véritable adresse de réponse de leurs messages. L'architecture du courrier électronique ne suppose pas qu'il y ait contact préalable entre l'expéditeur et le destinataire. Il n'est donc pas possible d'utiliser une authentification systématique. Le problème est de plus en plus préoccupant car des adresses falsifiées sont utilisées dans des escroqueries de hameçonnage qui trompent les destinataires afin de leur soutirer leurs numéros de cartes bancaires ou d'autres informations personnelles.

Cette technologie encore émergente souffre d'un manque de standardisation; elle consiste à marquer les messages dont le véritable expéditeur ne peut être vérifié. Un serveur de réception peut choisir de bloquer les messages non authentifiés mais la technologie ne l'oblige pas à procéder ainsi. La technologie ne fait que marquer le message. Le principal avantage de l'authentification au niveau du domaine est qu'elle réduira considérablement les faux positifs et permettra d'améliorer la fiabilité du filtrage basé sur la réputation. Le surcoût pour l'expéditeur est compensé par la garantie que le message sera distribué si l'expéditeur est authentifié et fait un usage légitime du système ou par le risque de responsabilité juridique en cas d'utilisation abusive d'une marque. Les détails spécifiques du processus de vérification varient selon le modèle choisi et plusieurs modèles d'authentification des serveurs existent actuellement. Parmi les plus répandus, citons SPF (*sender policy framework*) et Sender-ID.

Ces deux techniques peuvent être examinées ensemble parce qu'elles présentent un certain nombre de caractéristiques communes. Le choix de l'une ou de l'autre est toutefois moins évident.

SPF et Sender-ID peuvent être utilisées pour vérifier si un serveur de messagerie électronique est bien autorisé à expédier un message électronique pour le compte d'un domaine donné. Il faut pour cela publier un enregistrement dans le système de noms de domaines (DNS) qui donne la liste des serveurs de messagerie électronique autorisés pour un domaine donné. Les deux techniques diffèrent essentiellement sur le choix de l'identité sur laquelle porte le test. SPF teste le champ MAIL FROM de l'enveloppe [b-IETF RFC 2821], alors que Sender-ID teste les en-têtes [b-IETF RFC 2822].

Les administrateurs de serveurs prennent deux types de mesures: ils publient les enregistrements SPF dans le DNS et les testent à l'entrée. D'après un rapport récent [b-Lyris], en cas d'utilisation d'un enregistrement SPF incorrect, les chances de distribution d'un message sont désormais nettement réduites.

L'authentification du courrier électronique par vérification de l'adresse IP du serveur de l'expéditeur contribuera à réduire et à gérer le spam dans l'avenir. Cela nécessitera probablement la création de services qui complètent l'authentification: listes blanches privées, services de réputation et services d'accréditation, par exemple.

7.4.3 DKIM ou META

Les systèmes DKIM (*domainkeys identified mail*) et META (*message enhancements for transmission authorization*) sont utilisés pour authentifier le domaine de l'expéditeur au moyen d'une signature cryptographique automatiquement ajoutée par le serveur de messagerie électronique. L'authentification du courriel par signature cryptographique devrait contribuer à la réduction et à la gestion du spam dans l'avenir.

Le DKIM est le plus connu de ces modèles. Il fonctionne en imposant une signature numérique, ou clé privée, à tous les messages sortants. Les messages entrants sont authentifiés au niveau du domaine et du serveur de messagerie électronique en vérifiant que la clé privée correspond à la clé publique qui figure déjà sur le fichier. Cette méthode permet de s'assurer que le message vient forcément de l'ISP d'origine. Le DKIM est utile pour le domaine de l'expéditeur en ce sens qu'il permet de garantir la distribution aux ISP qui exécutent l'algorithme DKIM. Le DKIM a été récemment approuvé en tant que RFC par l'*Internet Engineering Task Force*, ce qui en fait une norme IETF.

7.5 Existence du domaine de l'expéditeur et demande de réponse

Nombreux sont les spammeurs qui opèrent à l'aide d'une adresse d'expéditeur non existante. Une règle peut être utilisée pour refuser ces messages, comme la directive reject_unknown_sender_domain de Postfix ou la directive BadMX de j-chkmail. Il est aussi possible de vérifier la validité de l'enregistrement du serveur entrant (MX) pour le domaine indiqué dans le champ "De:" du message. Certains spammeurs ont recours à un faux enregistrement MX pour éviter de recevoir des messages de protestation courroucées (par exemple, le MX pointe vers l'adresse 127.0.0.1, c'est-à-dire celle du PC local).

L'application de ces règles génère un volume modeste de trafic DNS, mais ce trafic aurait probablement existé du fait de la réponse; elle permet aussi de rejeter un certain volume de spam.

7.6 Existence d'un enregistrement de pointeur (PTR)

Un enregistrement PTR peut être inséré dans le DNS pour traduire sous forme de nom l'adresse IP du serveur de l'expéditeur, même s'il n'y a pas nécessairement vérification que ce nom correspond bien au domaine de l'expéditeur.

L'ajout de cet enregistrement n'est pas toujours contrôlé par le domaine de l'expéditeur (s'il n'y a pas de délégation addr.arpa par l'IP, par exemple) et ce dernier, même s'il est légitime, peut ne pas être en mesure de satisfaire à cette obligation. Ces enregistrements peuvent être utilisés pour rechercher la source d'un courriel et déterminer dans quelle mesure on peut avoir confiance. Ils peuvent aussi servir à déterminer si un courriel provient d'une adresse IP résidentielle ou à réexpédier un message d'erreur au bon serveur.

7.7 Listes noires et listes blanches

Le filtrage traditionnel et le suivi des plaintes déposées au sein de groupes d'utilisateurs peuvent à terme aboutir à la création de listes blanches d'expéditeurs acceptables et de listes noires d'expéditeurs suspectés d'être des spammeurs. La méthode des listes blanches et listes noires est souvent une solution trop radicale pour pouvoir être acceptée par la plupart des utilisateurs. La création des listes blanches prend du temps et une mise à jour continuelle est nécessaire. Les listes noires exigent également un suivi permanent. Chaque liste doit être assortie de mécanismes et de procédures de mise à jour pour corriger les faux positifs et traiter les plaintes frauduleuses

concernant les inscriptions sur la liste. L'usurpation d'identité (spoofing) et l'utilisation de relais ouverts peuvent aussi créer des problèmes liés à la source dont semble provenir le courriel.

Les listes noires consistent à recenser des sources de spam. Elles peuvent comprendre le nom des machines, les adresses IP et les adresses électroniques. Elles peuvent être tenues par une entité pour une utilisation partagée, à moins qu'elles ne soient créées et tenues à jour au niveau du serveur pour ses propres besoins.

Avec les agents de transfert de courrier (MTA) existants, ce test peut être effectué au niveau de la session SMTP et peut donc aboutir à un rejet avant même que le message soit envoyé. Certaines listes contiennent des relais ouverts qui n'envoient pas seulement du spam. Leur configuration en relais ouvert peut être considérée comme un comportement illégitime par les plates-formes auxquelles sont envoyés les messages.

Les listes noires varient considérablement en qualité, selon le degré de professionnalisme de celui qui les tient. Beaucoup sont mal gérées, abandonnées ou d'intégrité douteuse: les noms peuvent être ajoutés hâtivement, les critères appliqués ne sont pas forcément clairs et la radiation de la liste peut être quasiment impossible ou soumise à paiement. Ce problème s'explique principalement par l'absence d'un code de conduite ou d'une autre forme de réglementation pour organiser et limiter le fonctionnement des listes noires. Si cette solution doit être utilisée dans le futur, il faudra un effort coopératif pour établir une liste de bonnes pratiques, définissant clairement les cas où des adresses peuvent être inscrites en liste noire et les modalités de leur radiation.

Les listes noires contiennent inévitablement des erreurs qui empêchent certains messages légitimes de parvenir à leurs destinataires. Ce problème dit des faux positifs a donné lieu à des poursuites judiciaires, des expéditeurs légitimes estimant figurer par erreur sur la liste noire d'un ISP. De plus, le problème des faux positifs pour les utilisateurs individuels peut présenter l'inconvénient non négligeable de compter uniquement sur les technologies classiques de filtrage pour bloquer le spam. Toutefois, la plupart des mesures antispams peuvent conduire à des faux positifs. L'authentification au niveau du domaine devrait limiter ces faux positifs.

Si leur utilisation pose de nombreux problèmes, les listes noires constituent une solution rapide pour refuser la connexion avec des machines dont le comportement compromet la sécurité ou la qualité des services de la plate-forme à laquelle le courrier est envoyé, ou rejeter les messages provenant de certains expéditeurs.

7.8 Adresse du serveur expéditeur traitée comme "dynamique" ou "résidentielle"

Il s'agit d'une forme particulière de liste noire dans laquelle le critère d'inscription est le fait que l'adresse IP bloquée correspond non pas au serveur de messagerie électronique d'une organisation mais à la machine d'un abonné individuel à un ISP. L'idée est qu'un abonné ordinaire n'envoie pas de courrier directement au moyen du protocole SMTP, mais passe par le PTA de son fournisseur. Cela signifie que la machine bloquée envoie directement des messages de spam pour le compte d'un spammeur, ou plus généralement que les messages sont envoyés à l'insu du propriétaire de la machine (la machine a été corrompue et transformée en "zombie" pour envoyer les messages).

Les listes d'adresses de ce type ne sont pas toujours fiables car la plupart d'entre elles ont été compilées en fonction de critères heuristiques, comme la présence du terme "adsl" dans le nom de la machine. La gestion de ces listes mobilise aussi d'importantes ressources.

En revanche, certaines de ces listes, notamment celles compilées par le serveur qui les utilise, peuvent être utilisées pour faire la distinction entre les serveurs autorisés pour un domaine et les listes résidentielles. De plus, certains domaines publient les plages d'adresses résidentielles pour leur domaine.

Ce test peut être considéré comme une source de discrimination entre les "utilisateurs purs" et les fournisseurs. Ces derniers considèrent comme légitime la règle selon laquelle le propriétaire d'un

domaine refuse de connecter ses machines aux adresses résidentielles, car celles-ci constituent actuellement la principale source de spam. Mais les utilisateurs font valoir que le spam existe et qu'il faut protéger la liberté d'utiliser le courriel.

7.9 Les filtres

Le filtrage est la technologie antispam la plus répandue. Les principaux atouts des filtres sont la facilité de leur mise en œuvre et la latitude laissée aux utilisateurs de décider quels messages doivent être traités comme du spam. Les filtres heuristiques nécessitent que les utilisateurs donnent des critères, qui peuvent être des mots clés ou des adresses d'expéditeurs, qui déclenchent le filtre pour empêcher certains messages de parvenir jusque dans la boîte de réception de l'utilisateur. Il est facile pour les spammeurs d'utiliser des graphies délibérément fautives ou d'écrire les mots dans une langue différente pour contourner le filtrage par mots clés. Les filtres bayésiens sont fondés sur l'expérience. Ils produisent des statistiques sur les messages dans une table de reconnaissance à laquelle les utilisateurs individuels pourront par la suite se référer pour faire la distinction entre spam et courriels légitimes. Le filtre ne laisse alors passer que les messages qui s'apparentent aux courriels légitimes que l'utilisateur a reçus par le passé. Une étude menée en 2005 par la *Federal Trade Commission* des Etats-Unis d'Amérique [b-FTC] a montré que les filtres peuvent bloquer 90% du spam.

7.9.1 Filtres heuristiques

Ces filtres consistent à tester la présence dans le message de certaines caractéristiques typiques du spam, comme l'utilisation exclusive du HTML ou le type d'utilisateurs auxquels le message est adressé. Un processus d'apprentissage basé sur une série de courriels connus comme des spams et sur une série de courriels connus comme légitimes permet de procéder à une pondération (les notes ne sont donc pas calculées par un humain afin de réduire la subjectivité).

Le risque de ces filtres est que certains messages présentant des caractéristiques de spam (les messages spectaculaires en HTML, par exemple) seront traités comme du spam. De plus, il faut noter que les filtres mobilisent d'importantes ressources machine.

Ces filtres permettent de détecter une importante proportion de spam, et ne nécessitent ni apprentissage ni configuration. Mais ils utilisent un grand nombre de tests, et mieux vaut savoir qu'il est possible de choisir les tests à pratiquer ainsi que les notes à utiliser pour déterminer qu'un message est du spam.

7.9.2 Filtres par mots clés

Il s'agit de filtres binaires qui recherchent un mot clé (par exemple "viagra"). Le risque de faux positifs est très élevé et ces filtres sont très faciles à contourner: il suffit de rajouter un espace entre chaque caractère, d'intervertir des caractères ou d'utiliser des graphies fautives.

7.9.3 Filtres sur valeur de hachage

Les filtres sur valeur de hachage consistent à construire une valeur de hachage du message qui leur est soumis et à indiquer s'il a déjà été identifié comme étant du spam. Les faux négatifs sont fréquents: plusieurs types de spam ne sont pas identifiés, même lorsque le serveur les analyse à l'aide de filtres sur valeur de hachage. De plus, un message peut parfois varier suffisamment pour produire une valeur de hachage différente. L'une des solutions à ce problème est de différer le courriel (comme dans les listes grises). Les faux positifs sont rares.

7.9.4 Filtres bayésiens

Le principe de fonctionnement du filtre bayésien est de préparer le moteur en lui présentant une série de courriels identifiés comme du spam et une série de courriels identifiés comme légitimes; après un apprentissage du vocabulaire utilisé par les spammeurs à partir de ces courriels, le filtre

utilise les probabilités bayésiennes pour calculer si un message est du spam. Dans le cas d'un filtrage de groupe, l'apprentissage est généralement conduit par l'administrateur du système.

Ces filtres, qui s'appuient sur le concept de vocabulaire du spam, peuvent poser problème lorsqu'ils sont appliqués en environnement partagé. Dans un environnement d'échelle réduite et extrêmement uniforme (par exemple au sein d'une entreprise ou d'un département d'université, où chacun travaille dans le même domaine et utilise des vocabulaires voisins), cela peut fonctionner. Mais ce ne sera pas le cas pour un grand fournisseur de messagerie électronique et particulièrement pour un fournisseur public, sauf si la base partagée permet à chaque utilisateur individuel de personnaliser le filtre pour sa propre boîte de réception. Le problème est qu'un vocabulaire considéré comme acceptable par certains utilisateurs peut déclencher le filtre s'il a été qualifié de vocabulaire de spam au niveau du groupe.

Malgré les problèmes qu'ils peuvent poser au niveau du groupe, ces filtres sont extrêmement efficaces s'ils sont utilisés par des individus et constituent l'une des rares solutions qui, appliquée isolément, peut filtrer la quasi-totalité des courriels de spam après un apprentissage adapté.

7.9.5 Filtres comportementaux

Ce type de filtres examine le comportement du serveur distant, en regardant par exemple le nombre de courriels envoyés dans un intervalle de temps donné. La limitation du débit constitue un exemple de ce type de filtrage. L'idée est que les courriels ordinaires sont expédiés individuellement ou en très petit nombre, alors que les spams sont envoyés en très grand nombre.

Ce type de filtrage est extrêmement délicat car il n'y a généralement aucun moyen de faire la distinction entre un spammeur et un serveur de listes de diffusion légitime comme un forum de discussion.

D'après certains experts, il n'y a rien de choquant à ce qu'une plate-forme refuse certains volumes de courriels, essentiellement eu égard à ses propres dimensions ou au rôle de sécurité qu'elle doit assurer sur ses réseaux. Il n'est pas choquant de demander aux expéditeurs de courriels en grand nombre de respecter les ressources de la plate-forme distante en supportant le coût de la distribution de leurs messages sans essayer de les envoyer trop rapidement pour se défausser des coûts inhérents à l'utilisation du courriel comme mode de communication.

7.10 HELO/CSV

Un ordinateur d'expédition s'identifie par son nom à un ordinateur de réception au début de chaque transaction SMTP, au moyen de la commande SMTP "EHLO" ou "HELO".

Le service CSV (*certified server validation*) offre un dispositif permettant à un serveur de réception de courriels d'évaluer un serveur d'expédition de courriels. Il s'appuie sur une pratique existante des fournisseurs de service qui accréditent les réseaux depuis lesquels les systèmes expéditeurs se connectent.

La fonction HELO vérifie que le MTA distant est bien configuré, mais ces tests ne permettent pas de déterminer si l'expéditeur est un spammeur ou non. Les tests CSV ajoutent un test de probabilité sur le nom: correspond-il vraiment à un domaine? A la différence de SPF et de DKIM, CSV n'authentifie pas le domaine qui expédie le message, mais celui du serveur de courriel (qui peuvent être différents, par exemple dans le cas d'un fournisseur desservant un grand nombre d'utilisateurs).

Les directives de configuration (par exemple la directive reject_invalid_hostname de Postfix) testent le nom annoncé par le serveur. L'utilisation de tests HELO classiques entraîne le rejet d'un très grand nombre de messages légitimes. Toutefois, pour le moment, peu de sites savent modifier HELO pour qu'il fonctionne convenablement. Cette situation va probablement changer prochainement car des sites de plus en plus nombreux vont appliquer le test HELO, ce qui poussera à son amélioration.

7.11 Listes grises

Il s'agit d'envoyer délibérément un code d'erreur SMTP 4xx (erreur temporaire, par opposition à l'erreur définitive 5xx, voir [b-IETF RFC 2821]) lorsqu'on est en présence d'un nouvel expéditeur. Ce dernier, s'il s'agit d'un MTA normal, fera une nouvelle tentative d'expédition (généralement quinze minutes plus tard) et son message sera alors accepté. La plupart des logiciels de spam ne font pas de multiples tentatives d'expédition. Cette technique est extrêmement efficace et bloque tous les courriels de spam qui ne sont pas expédiés depuis un relais ouvert ou par le MTA d'un fournisseur. Elle empêche la réception de certains messages envoyés depuis des serveurs mal configurés et se prête particulièrement bien à une utilisation en conjonction avec une liste blanche.

7.12 Jetons et mots de passe

L'objet de ces techniques est d'inclure un mot de passe dans l'adresse à laquelle est envoyé le courriel ou d'utiliser un système défi-réponse de type test de Turing. Le logiciel du spammeur ne connaîtra pas le mot de passe et sera incapable de passer le test.

Ces techniques ne produisent pas de faux négatifs, sauf si les spammeurs décidaient d'employer des milliers de personnes à de très faibles salaires pour faire ce travail.

Un certain nombre d'utilisateurs légitimes vont refuser de passer le test ou en seront incapables. Il y aura donc beaucoup de faux positifs. Ces techniques ne sont intéressantes que pour les destinataires très connus qui reçoivent déjà de grandes quantités de courriels en masse (dont une partie de courriels légitimes), ou pour des destinataires qui souhaitent réduire le nombre de messages qu'ils reçoivent, ce qui relève de la liberté de communication. Il faut savoir également que tous les expéditeurs n'accepteront pas le test imposé. En sensibilisant les utilisateurs aux intérêts de cette technologie, on peut les inciter à passer les tests pour réduire le taux de non-acceptation.

7.13 Techniques diverses

Dans ce paragraphe, nous allons passer en revues différentes techniques, pour la plupart expérimentales ou insuffisamment testées.

7.13.1 Tests de l'enveloppe (BATV (*bounce address tag validation*) et SES (*signed envelope sender*))

Ces techniques sont encore récentes et leur déploiement est insuffisant pour qu'elles soient prises en considération.

7.13.2 Certification des courriels envoyés en masse – Réputation de l'expéditeur

Si une authentification efficace de l'expéditeur laisse aux ISP un rôle beaucoup plus simple dans le traitement du spam, l'authentification n'est qu'une étape préliminaire vers l'élimination du spam. Une fois que l'expéditeur peut être identifié, des facteurs tels que la réputation et l'accréditation sont nécessaires pour déterminer si un message doit être considéré comme du spam avant d'atteindre le destinataire. Des autorités indépendantes géreraient le processus de certification et fixeraient les critères. Un conseil de surveillance, comprenant une représentation plurisectorielle, superviserait les autorités de certification.

A cette fin, l'ePrivacy Group a établi la norme TEOS (*trusted email open standard*), fruit d'un programme d'autoréglementation du secteur privé, visant à séparer le courriel légitime du spam. TEOS va au-delà de l'authentification et crée une identité de confiance pour les expéditeurs de courriel à partir des signatures contenues dans les en-têtes. A la différence des signatures d'authentification du système DKIM, les signatures TEOS sont des "sceaux" visibles dans le message et certifient que l'expéditeur remplit les critères spécifiés.

Pour atténuer le problème des courriels expédiés en masse qualifiés à tort de spam, les acteurs du secteur privé continuent d'examiner l'efficacité d'un mécanisme de certification pour le courriel

expédié en masse. Par exemple, les courriels en masse légitimes pourraient être identifiés au niveau de l'ISP par une étiquette reconnue par le serveur, ce qui permettrait une utilisation plus fiable des filtres de courriels. Plusieurs critères pourraient être retenus dans le paramétrage du processus de certification, par exemple l'engagement à se conformer à des pratiques strictes en matière de respect de la vie privée. Par exemple, la France travaille avec son agence de protection des données, la Commission nationale de l'informatique et des libertés (CNIL), sur un projet de certification des expéditeurs qui notifient l'utilisation de fichiers clients.

Chaque ISP tiendrait une liste blanche de clients certifiés. Cette proposition exige un accord entre ISP sur le processus de certification et ne nécessite pas d'intervention extérieure. Mais pour que cette méthode soit efficace, il faudrait une masse critique d'ISP, et une confiance entre ISP, puisqu'il n'y a pas de supervision extérieure du processus de certification. De plus, il peut être délicat de fixer un nombre donné pour définir les envois en masse. Des spammeurs astucieux pourraient utiliser un grand nombre de comptes de messagerie électronique gratuits pour envoyer des volumes importants de spam, en veillant à ce que le nombre de message envoyés depuis chaque compte soit tout juste inférieur au seuil prédéfini pour l'envoi en masse.

7.13.3 Validation du serveur de l'expéditeur

A étudier.

7.13.4 Signatures PGP

A étudier.

7.13.5 Configuration du système

Les bonnes pratiques de sécurité pour les entreprises et les particuliers en matière de ports, de pare-feu, de réseaux, de routeurs, de proxys, d'accès, de mots de passe, de protection des clés d'autorisation et d'installation de logiciels constituent des exemples d'utilisation de la configuration du système comme technologie antispam. En configurant son système de manière à bloquer les courriels non sollicités, on n'intercepte qu'un certain pourcentage de spam. A mesure qu'un nombre croissant de systèmes se dotent de tels mécanismes, les spammeurs deviendront certainement de plus en plus ingénieux, mais en même temps, plus il y a d'obstacles à surmonter, moins il devient intéressant d'envoyer du spam. Aujourd'hui, les gens envoient du spam parce que c'est simple, rapide et très peu onéreux. Avec le temps cela le sera de moins en moins – des centaines de milliers d'administrateurs systèmes y travaillent – et il sera plus difficile d'atteindre son but par le spam.

7.13.6 Outils antivirus

Les antivirus sont des outils importants pour réduire le risque d'infection des systèmes informatiques par des courriels de spam. Généralement, les spams nocifs sont accompagnés de fichiers qui peuvent déclencher des virus. Les logiciels antivirus analysent les boîtes de courriel et préviennent les infections virales.

Un certain nombre d'ISP surveillent et actualisent en permanence les interfaces API (interface de programmation d'application) des antivirus, ou VSAPI, avec Exchange Server. Cette technologie consiste à effectuer l'analyse antivirus au niveau des boîtes de messagerie des utilisateurs, afin d'effectuer l'analyse hors du périmètre du réseau et réduire ainsi l'impact des virus et des courriers infectants sur les infrastructures de réseau. Il est aussi possible d'empêcher les courriels infectés de quitter une organisation en analysant non seulement le courriel entrant, mais aussi le courriel sortant.

7.14 Comment utiliser cette revue de technologies et quels facteurs prendre en compte?

L'utilité d'un outil quel qu'il soit dépendra des besoins, de la capacité technique et de l'infrastructure de l'utilisateur de cet outil. Les outils sont conçus pour être mis en place en différents points du système et avec des finalités différentes. Les utilisateurs devront analyser en profondeur leurs

besoins et leurs stratégies de défense pour choisir et mettre en œuvre leurs outils antispams. Les outils eux-mêmes ne sont pas non plus identiques en termes de maturité, d'efficacité, de fiabilité et de simplicité de mise en œuvre. Certains outils produiront davantage de faux positifs, certains sont particulièrement efficaces dans certains domaines et certains sont plus dispendieux que d'autres en termes de coût, d'utilisation de l'infrastructure, de bande passante ou de capacité et demandent davantage d'expertise technique. Nous avons énuméré quelques-uns de ces facteurs, mais les utilisateurs devront évaluer les outils dans le contexte de l'application spécifique envisagée.

Quelques-uns des tests que nous avons évoqués ont pour but de lutter contre le spam, alors que d'autres visent à empêcher certains comportements qui représentent une menace contre la sécurité, qui ne respectent pas les ressources de la plate-forme de destination, ou simplement ne se conforment pas aux règles acceptées régissant l'envoi de messages électroniques. Lorsqu'une règle est appliquée après réception des données qui constituent le message expédié, il reste à déterminer comment sera traité le message. Cela dépendra bien sûr des résultats des tests pratiqués. Certains tests sont plus fiables que d'autres et peuvent donc justifier le recours à des mesures plus radicales. De plus, il peut être décidé de pratiquer d'autres tests plus onéreux sur certains messages.

Nous allons voir maintenant les différentes possibilités de traitement des messages en fonction du point où est appliquée la règle.

7.15 Rejet au niveau de la session SMTP

L'intérêt du rejet à ce niveau réside dans la non-prise en charge du message électronique, dont la distribution reste sous la responsabilité du serveur distant, lequel est informé de la situation. De plus, cette solution économise de la bande passante, d'abord parce que le message n'est pas reçu, et ensuite parce que le serveur distant n'aura pas besoin d'envoyer une notification de statut de distribution (DSN) (message généré en réponse à un rejet, voir [b-IETF RFC 3461]) que peut générer le message. La tâche d'envoyer le message d'échec de l'envoi est transférée à l'expéditeur.

Toutefois, avec ce type de rejet, il n'est pas possible de conserver une copie du message (et donc de récupérer un message légitime qui n'aurait pas été accepté, ou simplement d'enquêter sur un rejet).

De plus, tous les serveurs SMTP ne sont actuellement pas capables de pratiquer certains tests au cours de la session SMTP. Ce point est en passe de changer, avec la diffusion croissante de nouveaux produits et en particulier d'interfaces comme "milter" de Sendmail, "policy server" de PostFix, et prochainement OPES, qui pourra faire fonctionner tous les programmes avec la session SMTP.

7.16 Rejet muet

Cette méthode est souvent déconcertante pour l'utilisateur lambda qui s'attend à ce que son courriel soit distribué ou au moins à ce qu'un rejet lui soit notifié. Le principe "distribuer ou notifier" est une règle cardinale du courrier électronique, mais devra probablement être abandonné en raison du grand nombre de courriels censés être envoyés par un utilisateur qui en réalité n'y est pour rien.

Idéalement, il faudrait conserver une trace des courriels détruits de cette manière, afin de permettre l'application de techniques comme celle du suivi des messages, par exemple en mettant en œuvre la norme [b-IETF RFC 3885], qui décrit le protocole de suivi des messages, permettant aux utilisateurs de connaître le parcours de leur message (comme les systèmes de suivi des colis des sociétés de transport).

7.17 Rejet avec envoi de DSN (notification de statut de distribution ou "retour à l'envoyeur")

C'est la méthode traditionnellement utilisée pour le courrier électronique. Mais, en raison de l'existence de joejobs, il existe un risque de pénaliser des expéditeurs innocents, comme avec les programmes antivirus qui envoient des DSN à tort.

7.18 Distribution dans une boîte de réception réservée au spam

Quand peu de messages sont bloqués au niveau de l'entrée sur la plate-forme, la boîte de spam peut contenir beaucoup de messages, ce qui dissuade les utilisateurs de les lire. Le message n'est pas détruit, mais l'utilisateur a la possibilité de rectifier les faux positifs.

7.19 Marquage

Le serveur ne prend pas de décision mais place simplement une note sur le courriel. Cette technique laisse le plein contrôle à l'utilisateur mais contraint aussi l'utilisateur à télécharger le spam.

Notons qu'un fournisseur de messagerie électronique peut laisser l'utilisateur choisir si le courriel incriminé sera marqué ou distribué dans la boîte de spam. Cette solution est relativement simple à gérer.

Appendice I

Activités de lutte contre le spam par courrier électronique

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

I.1 Introduction

Le présent appendice décrit les activités récentes menées dans divers organismes (notamment l'UIT-T), les spécifications techniques ainsi que les alliances et les initiatives du secteur privé concernant la lutte contre le spam par courrier électronique. Les organismes recensés ici participaient activement à la lutte contre le pourriel au moment de l'élaboration de la présente Recommandation. L'ensemble des spécifications techniques et leur validité ainsi que la situation des organismes recensés pourront évoluer dans l'avenir.

I.2 Activités internationales de lutte contre le spam

I.2.1 UIT

Dans la Déclaration de principes adoptée pendant la première phase du Sommet mondial sur la société de l'information (SMSI), tenue à Genève en décembre 2003 [b-SMSI-2003], le spam a été identifié comme une menace potentielle à l'encontre de la pleine utilisation des services Internet et de courrier électronique. Reconnaissant que le spam est un "problème important et qui ne cesse de s'aggraver pour les utilisateurs, les réseaux et l'Internet dans son ensemble", les participants au SMSI ont estimé nécessaire de "prendre des mesures appropriées, au niveau national et international" afin de fiabiliser et de sécuriser l'utilisation des TIC.

Les Etats Membres de l'UIT ont manifesté leur intérêt pour les questions touchant au spam lors de l'Assemblée mondiale de normalisation des télécommunications (AMNT) de l'UIT qui a eu lieu à Florianópolis (Brésil) en octobre 2004. Au cours de l'Assemblée, les Membres de l'UIT ont approuvé deux résolutions sur les activités futures de l'UIT dans le domaine du spam.

Dans la première, à savoir la Résolution 51 sur la lutte contre le spam, les Directeurs des trois Secteurs de l'UIT et le Secrétaire général ont été chargés d'établir d'urgence un rapport à l'intention du Conseil, à sa session de 2005, sur les initiatives pertinentes prises par l'UIT et sur les autres initiatives internationales en vue de lutter contre le spam et de proposer – avec la contribution des Etats Membres et des Membres de Secteur – des mesures de suivi possibles pour examen par le Conseil. Par ailleurs, les Etats Membres ont été invités à prendre des dispositions appropriées au sein de leur cadre juridique national pour veiller à ce que soient adoptées des mesures indiquées et efficaces de lutte contre le spam.

La seconde Résolution, à savoir la Résolution 52 sur la lutte contre le spam par des moyens techniques, stipule que "le pollupostage [spam] pose des problèmes de sécurité pour les réseaux de télécommunication, et constitue notamment un véhicule pour les virus, vers informatiques, etc.". Dans cette Résolution, il est également reconnu que les Recommandations pertinentes de l'UIT-T fournissent des indications qui pourraient être utiles aux développements futurs dans ce domaine. Les commissions d'études compétentes de l'UIT-T ont donc été chargées – en coopération avec l'*Internet Engineering Task Force* (IETF) et les autres groupes concernés – d'élaborer d'urgence des Recommandations techniques sur la lutte contre le spam, selon qu'il conviendra, et de rendre régulièrement compte au Groupe consultatif de la normalisation des télécommunications des progrès accomplis. Quant au Directeur du Bureau de la normalisation des télécommunications, il a été chargé d'apporter toute l'assistance nécessaire et de communiquer au Conseil de l'UIT les résultats obtenus.

I.2.2 OCDE

Le spam a un impact négatif sur l'économie du numérique et entraîne des coûts économiques et sociaux importants pour les pays de l'OCDE comme pour les autres économies. Face aux nouveaux problèmes qui pourraient se poser avec la convergence des technologies de la communication et l'émergence des télécommunications ubiquitaires et de l'Internet mobile, les pays membres de l'OCDE sont confrontés à la nécessité de trouver des solutions pour éliminer le spam. Pour relever ce défi, le Comité de la politique de l'information, de l'informatique et des communications (Comité PIIC) de l'OCDE, lors de sa réunion des 3 et 4 mars 2003, a décidé que des travaux prioritaires devaient être consacrés à cet important dossier, notant que le problème était d'ampleur mondiale. Le Comité de la politique à l'égard des consommateurs (CPC) a également exprimé son intérêt pour la poursuite de travaux sur ce thème dans le cadre de l'OCDE. Les problèmes liés au spam ont fait l'objet d'une première étude exploratoire dans un document de référence et dans le cadre d'un atelier sur le spam qui s'est tenu sous l'égide de la Commission européenne, à Bruxelles, en février 2004.

Le spam a des conséquences sur plusieurs plans. Il pose ainsi des problèmes d'utilisation et d'encombrement des réseaux et des problèmes liés aux réseaux IP, des problèmes de respect de la vie privée et de sécurité des réseaux, et des problèmes de protection des consommateurs. Afin de mieux coordonner les travaux sur le spam et de parvenir plus rapidement à un consensus sur un cadre d'action pour la lutte contre les problèmes causés par ce phénomène, le Conseil de l'OCDE a décidé en juillet 2004 de créer un "Groupe de réflexion transversal sur le spam". Ce Groupe de réflexion était invité à faire rapport aux comités CPC et PIIC avant juillet 2006.

L'objectif premier du Groupe de réflexion était de rassembler toutes les personnes chargées de coordonner les politiques de lutte contre le spam afin de préparer le plus efficacement possible les outils dont les pouvoirs publics avaient un besoin urgent pour lutter contre le spam, grâce à une approche plus large du problème et à l'expertise pluridisciplinaire de l'OCDE.

Le Groupe de réflexion avait pour mission d'étudier, de documenter et de faire connaître la gamme des stratégies antispams existantes et émergentes dans tous les secteurs. Sachant qu'il n'existe pas de remède miracle qui peut à lui seul venir à bout du spam, le Groupe de réflexion a élaboré en avril 2006 une "Boîte à outils antispams" reposant sur le principe selon lequel il faut mobiliser de façon coordonnée plusieurs éléments différents pour favoriser le développement de stratégies et solutions de lutte contre le spam - techniques, réglementaires et d'application de la loi –et faciliter la coopération internationale face à ce problème. La Boîte à outils antispams de l'OCDE a donc pour but de rassembler une série cohérente de mesures complémentaires et d'autres initiatives (notamment coercitives). L'élaboration et la mise en œuvre de la Boîte à outils s'appuient essentiellement sur les apports des parties prenantes dans les différents domaines concernés. Elle se compose de huit éléments interdépendants:

– Réglementation antispam
– Coopération internationale pour la répression du spam
– Solutions antispams pilotées par le secteur privé
– Technologies antispams existantes et émergentes
– Education et sensibilisation
– Partenariats de coopération contre le spam
– Mesure du spam
– Coopération mondiale (ouverture)

Des documents de référence ont été rédigés pour le Groupe de réflexion sur plusieurs éléments de la Boîte à outils. Le présent Appendice fait la synthèse des travaux menés par le Groupe de réflexion et de leurs conclusions. Il est complété par la recommandation du Conseil de l'OCDE relative à la coopération transfrontière dans l'application des législations contre le spam et par le site web de l'OCDE sur la lutte contre le spam (www.oecd-antispam.org).

I.2.3 APEC

Au sein de l'Organisation de coopération économique Asie-Pacifique (APEC), les problèmes liés au spam sont examinés par le groupe de travail sur les télécommunications et l'information (Groupe de travail TEL). Ce Groupe s'emploie à améliorer l'infrastructure des télécommunications et de l'information dans la région et à faciliter une coopération efficace, la liberté dans le commerce et dans les investissements et un développement durable.

Dans le domaine de la sécurité des réseaux et de l'infrastructure, le Groupe de travail TEL collabore avec d'autres organismes sur les questions de sécurité et renforce ses travaux en vue de la création d'un environnement en ligne sûr dans la société de l'information, s'intéressant à des problèmes tels que le spam, pour lutter contre les menaces qui visent les réseaux; en particulier il mène des actions de suivi concernant les principes de l'APEC en matière de lutte contre le spam et les lignes directrices de l'APEC en matière de mise en œuvre de la lutte contre le spam et il coopère avec des organismes internationaux ou régionaux tels que l'UIT, l'OCDE et l'Association des nations de l'Asie du Sud-Est (ANASE). On trouvera des informations sur le sujet sur le site web du Groupe de travail TEL de l'APEC (http://www.apectelwg.org/).

I.3 Elaboration de spécifications techniques sur la lutte contre le spam

I.3.1 UIT-T

Dans sa Résolution 52, l'Assemblée mondiale de normalisation des télécommunications (Florianópolis, 2004) a chargé les commissions d'études compétentes, en coopération avec l'IETF et les autres groupes concernés, d'élaborer des Recommandations techniques sur la lutte contre le spam, y compris les définitions nécessaires, selon qu'il conviendra, et de rendre régulièrement compte au Groupe consultatif de la normalisation des télécommunications des progrès accomplis.

La Commission d'études 17, qui est la Commission d'études directrice sur la sécurité des télécommunications et qui mène les activités demandées au titre des Résolutions 50, 51 et 52 de l'AMNT, est bien placée pour étudier la palette des mesures techniques possibles pour lutter contre le spam en lien avec la stabilité et la robustesse des réseaux de télécommunication. La CE 17 de l'UIT-T a créé un Groupe du Rapporteur spécialisé, sur la Question 17/17, chargé d'élaborer des solutions techniques de lutte contre le spam. Initialement destinés à établir des spécifications techniques sur la lutte contre le spam par courrier électronique (pourriel), les travaux s'orienteront ensuite vers l'élaboration de solutions techniques sur la lutte contre le spam dans les applications multimédias IP telles que la téléphonie IP, la messagerie instantanée, etc. Les spécifications techniques portent ou vont porter sur les lignes directrices, les exigences, les cadres techniques et les moyens techniques de la lutte contre les divers types de spam.

I.3.2 IETF

L'IETF a élaboré les divers documents RFC suivants sur la lutte contre le pourriel, contenant des lignes directrices et des spécifications techniques:

– [b-IETF RFC 2505] "Antispam Recommendations for SMTP MTAs":

  Ce document donne un certain nombre de recommandations sur la mise en œuvre des agents MTA (agents de transfert de courrier) dans le protocole SMTP afin d'améliorer leur capacité à réduire les incidences du spam. L'objectif est que ces recommandations soient appliquées à un nombre suffisant d'agents MTA SMTP dans l'Internet pour venir à bout du spam plus facilement et que les divers fournisseurs d'agents MTA utilisent ces recommandations comme des lignes directrices. Il ne s'agit pas d'une solution finale, mais l'inclusion et l'utilisation de ces recommandations dans tous les agents MTA SMTP présents dans l'Internet permettraient d'améliorer considérablement les choses et de laisser du temps pour concevoir une solution à plus long terme. La partie consacrée aux travaux futurs donne quelques idées qui pourront être intégrées dans une telle solution à long terme. Toutefois, il se peut très bien que la solution ultime ne soit pas de nature technique mais

sociale, politique, ou juridique. L'implémenteur doit savoir que plusieurs des méthodes proposées pourraient conduire à un risque accru concernant les attaques par déni de service. Par exemple, l'augmentation du nombre des requêtes adressées aux serveurs DNS et de la taille des fichiers de journalisation pourrait déboucher sur une surcharge, voire une panne, des systèmes pendant une attaque.

– [b-IETF RFC 2635] "*DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*)*"

  Ce document explique pourquoi les messages électroniques de masse non sollicités sont nuisibles dans le domaine des réseaux. Il contient un ensemble de lignes directrices sur le traitement des messages non sollicités, à l'intention des utilisateurs, des administrateurs de système, des administrateurs des actualités et des gestionnaires de listes de diffusion. Il formule en outre des suggestions que les fournisseurs de services Internet sont invités à suivre.

– [b-IETF RFC 3685] "*SIEVE Email Filtering: Spamtest and VirusTest Extensions*":

  Les extensions SIEVE 'spamtest' et 'virustest' permettent aux utilisateurs, grâce à des commandes portables simples, de vérifier la présence de spam ou de virus dans les messages électroniques. Chaque extension offre un nouveau test qui fonctionne par comparaison avec des 'notes' numériques. Il appartient à l'implémentation SIEVE sous-jacente de procéder aux vérifications effectives pour réaliser correctement les tests.

– [b-IETF RFC 4686] "Analysis of Threats Motivating DomainKeys Identified Mail (DKIM)"

  Ce document analyse certaines menaces contre le courrier Internet auxquelles l'authentification de courrier fondée sur la signature devrait pouvoir apporter une solution, en particulier l'authentification DKIM (*domainkeys identified mail*). Il porte sur la nature et l'emplacement des pirates, sur leurs capacités et sur le but recherché de leurs attaques.

En plus de ces documents, il existe plusieurs projets en cours sur l'authentification au niveau du domaine afin de lutter contre le pourriel.

I.4 Liste d'alliances et d'initiatives du secteur privé concernant la lutte contre le spam

On trouvera ci-dessous une liste d'initiatives du secteur privé dans le monde entier. Non exhaustive, cette liste vise à illustrer la grande diversité des projets entrepris par diverses organisations afin de combattre le spam de manière plus coordonnée et plus efficace.

I.4.1 Anti-Phishing Working Group

L'*Anti-Phishing Working Group* (APWG) [b-APWG] est une association mondiale regroupant tous les acteurs du secteur privé et les organismes d'application de la loi, dont la mission est de venir à bout de la fraude et du vol d'identité qui résultent du problème croissant de l'hameçonnage, du détournement de domaine et de l'imitation de courrier électronique. L'organisation permet d'examiner le problème de l'hameçonnage, elle définit l'ampleur du problème en termes de coûts essentiels et de coûts accessoires et diffuse des informations et des bonnes pratiques afin de résoudre le problème. Lorsqu'elle le juge utile, elle communique ces informations aux organismes d'application de la loi.

I.4.2 Authentication and Online Trust Alliance

Fondé en octobre 2004, l'*Email Authentication.org* est devenu ensuite l'*Authentication and Online Trust Alliance* (AOTA Inc.). L'AOTA a pour mission de renforcer la confiance en ligne dans toutes les formes de messagerie électronique, le commerce électronique, la banque en ligne et l'Internet, contribuant ainsi à améliorer la sécurité et la protection en ligne tant des entreprises que des particuliers. Les objectifs sont notamment de faciliter l'application de bonnes pratiques, le partage de données, la mise en œuvre de normes et de solutions concernant l'authentification, l'identité et la

réputation dans le courrier électronique et dans l'Internet et le déploiement de stratégies de défense des domaines, par la fourniture d'avis normatifs et fondamentaux dans un environnement indépendant du fournisseur. L'AOTA est constituée de grandes entreprises et d'organisations sans but lucratif, qui cherchent à améliorer la confiance dans la messagerie électronique, l'Internet et le commerce électronique. Compte tenu du grand nombre de courriels hameçons et de courriels trompeurs, cette collaboration est essentielle pour aider à garantir la fiabilité et la possibilité de distribution des messages électroniques, renforcer la confiance en ligne et protéger les marques et les domaines des entreprises dans le monde entier.

Début 2004, un groupe d'acteurs du secteur privé de premier plan dirigé par Bigfoot Interactive, Email Sender and Provider Coalition (ESPC), Microsoft et Sendmail ont commencé à se réunir afin de rechercher des solutions pour authentifier les messages électroniques et améliorer la confiance des utilisateurs. Après un sommet sur l'authentification tenu par la *Federal Trade Commission* des Etats-Unis d'Amérique en novembre 2004, qui a été cofinancé par le *National Institute of Standards and Technology* du département du commerce, il a été décidé de prendre des mesures énergiques pour faire progresser les travaux au sujet de l'authentification des messages électroniques; c'est alors que le site emailauthentication.org a été créé. Compte tenu du nombre toujours aussi grand de courriels hameçons et de courriels trompeurs, ayant pour effet d'ébranler la confiance des particuliers et des entreprises, l'emailauthentication.org est devenu en septembre 2006 l'AOTA.

L'AOTA est toujours spécialisée dans l'authentification des courriers électroniques, domaine dans lequel cette organisation continue à posséder une hégémonie technique, mais sa mission a été élargie afin d'examiner des questions plus générales et de remédier aux menaces qui ont une incidence sur la confiance en ligne.

I.4.3 Réseau de contact des autorités antispam

La Commission européenne est à l'origine de la création d'un groupe officieux, appelé "réseau de contact des autorités antispam (CNSA)", constitué des autorités nationales intervenant dans l'application de l'Article 13 de la directive vie privée et communications électroniques (2002/58/EC).

Dans le cadre du CNSA, des informations sur les pratiques actuelles de lutte contre le spam sont échangées entre les autorités nationales, y compris les bonnes pratiques en matière de réception et de traitement des plaintes et d'autres renseignements pertinents ainsi qu'en matière d'enquête sur le spam et de lutte contre ce fléau. La Commission assure le secrétariat du CNSA. Le CNSA bénéficie en outre de l'aide d'un coordonnateur, qui facilite l'échange d'informations entre les membres du CNSA et aide la Commission à assurer le secrétariat. Le coordonnateur actuel est le bureau du premier ministre français. Le CNSA se réunit régulièrement (3 à 4 fois par an) à Bruxelles. Par ailleurs, une réunion conjointe du CNSA et du Plan d'action de Londres a lieu chaque année.

Le CNSA a élaboré une procédure de coopération visant à faciliter la transmission des plaintes et d'autres renseignements pertinents entre autorités nationales.

I.4.4 Digital PhishNet

Le *Digital PhishNet* (DPN), créé le 8 décembre 2004, vise à faire en sorte que les leaders du secteur privé œuvrant dans les domaines des technologies, de la banque, des services financiers et des enchères en ligne s'unissent aux organismes d'application de la loi afin de combattre l'"hameçonnage", qui est une forme de vol d'identité en ligne destructrice de plus en plus répandue.

L'hameçonnage est une nouvelle menace en ligne insidieuse et particulièrement nuisible qui consiste à diriger les utilisateurs vers de faux sites web, généralement au moyen de courriels d'apparence légitimes, pour leur soutirer des informations personnelles et financières telles que des numéros de carte de crédit et des mots de passe. Si d'autres groupes du secteur privé se concentrent sur l'identification des sites web hameçons et sur le partage de bonnes pratiques et d'informations sur des cas concrets, le DPN est le premier groupe de son genre à veiller surtout à apporter son aide

dans l'application du droit pénal et dans l'arrestation et la poursuite de ceux qui commettent des infractions pénales contre les utilisateurs par le biais de l'hameçonnage. La voie de communication établie par le DPN entre le secteur privé et les organismes d'application de la loi étant simple et unifiée, les données essentielles pour la lutte contre l'hameçonnage peuvent être compilées et communiquées aux organismes d'application de la loi en temps réel.

I.4.5 Email Sender and Provider Coalition

L'*Email Sender and Provider Coalition* (ESPC) est un groupe de leaders du secteur privé qui, ensemble, cherchent des solutions à la prolifération persistante du spam et au nouveau problème de la possibilité de distribution. Les membres de l'ESPC reconnaissent la nécessité de disposer de solutions antispams robustes garantissant la distribution du courrier électronique légitime et participent activement à la lutte contre le spam. L'ESPC cherche des solutions aux problèmes du spam et de la possibilité de distribution en combinant défense des droits, progrès techniques et normes du secteur privé.

L'ESPC comporte quatre sous-comités:

– Législation – donne des orientations sur les pressions exercées par l'ESPC concernant la législation fédérale et d'état en matière de spam.

– Relations avec les destinataires – facilite une meilleure compréhension et la poursuite du dialogue entre la communauté des expéditeurs et celle des destinataires.

– Technologies – évalue et développe des solutions techniques plus ciblées concernant le spam (et donnant moins de faux positifs). Un groupe de travail technique a été créé au sein de ce sous-comité afin d'examiner et de proposer de telles solutions. Ce groupe se réunit en fonction des besoins, des réunions présentielles étant parfois programmées.

– Communications – définit la stratégie générale de l'ESPC en matière de relations publiques.

I.4.6 Institute for Spam and Internet Public Policy

L'*Institute for Spam and Internet Public Policy* (ISIPP) procède à des analyses, fournit des informations et mène des consultations sur des problèmes rencontrés par le secteur privé en ce qui concerne les politiques publiques et les processus applicables au spam, au courrier électronique, à la possibilité de distribution du courrier électronique et à l'Internet. L'ISIPP offre aussi un service d'accréditation des expéditeurs de courrier électronique, SuretyMail, qui est largement utilisé. De plus, il organise et finance des forums du secteur privé, par exemple des tables rondes sur la gestion du courrier électronique, des sommets sur la possibilité de distribution du courrier électronique et des conférences sur le droit associé à l'Internet.

I.4.7 Plan d'action de Londres

Le Plan d'action de Londres est un réseau mondial de représentants d'organismes d'application de la loi et du secteur privé engagés dans la lutte contre le spam, l'hameçonnage et les menaces en ligne associées. La *Federal Trade Commission* des Etats-Unis d'Amérique et l'*Office of Fair Trading* du Royaume-Uni ont été à l'origine de la création du Plan d'action de Londres en 2004. Ce Plan compte désormais des membres dans plus de 20 pays. Depuis sa création, il encourage des relations bilatérales et multilatérales entre les organismes d'application de la loi, facilitant ainsi une coopération internationale dans plusieurs enquêtes sur le spam. En 2005, il a collaboré avec plusieurs autres partenaires du secteur public pour mener l'opération "*Operation Spam Zombie*", une initiative qui visait à ce que des organismes du monde entier envoient des lettres aux fournisseurs de services Internet pour leur demander instamment d'employer des mesures de protection afin d'éviter que les ordinateurs des utilisateurs soient détournés pour envoyer des spams.

Comme indiqué plus haut, une réunion conjointe du Plan d'action de Londres et du CNSA a lieu chaque année. Récemment, le Plan d'action de Londres a tenu son troisième atelier conjoint avec le CNSA du 9 au 11 octobre 2007 à Washington, D.C. Cet atelier s'est déroulé parallèlement à la

11ème réunion générale du MAAWG. Plusieurs séances conjointes du Plan d'action de Londres, du CNSA et du MAAWG ont été consacrées à un grand nombre de sujets pertinents.

Pendant l'atelier de 2007, le Plan d'action de Londres a également dispensé des cours de formation pour les organismes d'application de la loi, il a étudié les avantages présentés par les initiatives de coopération public-privé et il a examiné les possibilités de renforcer la coopération transfrontière en matière d'application de la loi. Des représentants d'organismes d'application de la loi et du secteur privé issus de plus de 20 pays ont participé à l'atelier conjoint.

I.4.8 Messaging Anti-Abuse Working Group

Le *Messaging Anti-Abuse Working Group* (MAAWG) est une organisation mondiale qui cherche à préserver la messagerie électronique contre les usages abusifs et les exploits en ligne afin d'améliorer la confiance de l'utilisateur, tout en garantissant la possibilité de distribution des messages légitimes. Basé sur un grand nombre de fournisseurs de services Internet et d'opérateurs de réseau représentant plus de 600 millions de boîtes de courrier électronique, de fournisseurs de technologies clés et d'expéditeurs, le MAAWG s'emploie à remédier aux usages abusifs de la messagerie par le biais d'initiatives dans trois domaines: technologies, collaboration avec le secteur privé et politiques publiques.

La mission du MAAWG est de rassembler les acteurs concernés par la messagerie afin de collaborer pour venir à bout des formes d'usage abusif de la messagerie comme le pourriel, les attaques par virus, les attaques par déni de service, etc. Pour cela, le MAAWG lance des initiatives dans les trois domaines nécessaires pour résoudre le problème de ces usages abusifs de la messagerie: collaboration, technologies et politiques publiques.

I.4.9 *Spamhaus*

Le *Spamhaus* est une organisation internationale sans but lucratif dont la mission est de repérer les spammeurs, les gangs de spammeurs et les services non sollicités, d'assurer une protection antispam en temps réel fiable pour les réseaux IP, de collaborer avec les organismes d'application de la loi pour identifier et poursuivre les spammeurs dans le monde entier et d'exercer des pressions sur les pouvoirs publics en vue de légiférer efficacement contre le spam. Créé en 1998, le *Spamhaus* est basé à Genève (Suisse) et à Londres (Royaume-Uni) et fonctionne avec une équipe spécialisée de 25 enquêteurs situés dans neuf pays.

Le *Spamhaus* publie le *Register Of Known Spam Operations* (ROKSO) – une base de données rassemblant des informations et des preuves sur les '200' pires gangs de spammeurs connus dans le monde entier, qui est utilisée par les fournisseurs de services Internet pour éviter que des spammeurs connus fassent une utilisation abusive de leurs réseaux ainsi que par les organismes d'application de la loi pour aider à traquer les spammeurs professionnels et à engager des poursuites à leur encontre.

Le *Spamhaus* publie un certain nombre de bases de données de blocage du spam en temps réel (*Spamhaus Block List* (SBL), *Exploits Block List* (XBL) et *Policy Block List* (PBL)). Diffusées depuis un réseau de 40 serveurs DNS dans 17 pays, les listes de blocage du *Spamhaus* sont utilisées par un grand nombre de fournisseurs de services Internet, entreprises, universités, pouvoirs publics et réseaux militaires.

Les activités sont financées par des sponsors et des donateurs. L'infrastructure internationale est financée sur la fourniture d'un service de synchronisation des listes de blocage du spam ('*Spamhaus Data Feed*') offert par une organisation distincte aux grands opérateurs de réseaux IP et aux sociétés de filtrage du spam.

I.4.10 *StopSpamAlliance*

La *StopSpamAlliance* est une initiative conjointe de l'APEC, du CNSA de l'UE, de l'UIT, du Plan d'action de Londres, de l'OCDE et du Groupe antispam Séoul-Melbourne, qui vise à rassembler des informations et des ressources pour combattre le spam.

Conformément à l'Agenda de Tunis du SMSI [b-SMSI-2005] – demandant aux membres de "traiter efficacement le problème toujours plus préoccupant du spam" et demandant à toutes les parties prenantes d'adopter une approche concertée pour lutter contre le spam – les pages de la *StopSpamAlliance* contiennent des liens vers des initiatives dans les domaines de la promulgation de lois contre le spam et de leur application, de la sensibilisation des particuliers et des entreprises, de la mise en œuvre de bonnes pratiques et de la coopération internationale.

Un calendrier commun des manifestations, décrivant les manifestations internationales sur la lutte contre le spam et les menaces associées, organisées par les organisations participantes, est également disponible. L'adresse du site web est la suivante: http://stopspamalliance.org/.

I.4.11 *Trusted Electronic Communications Forum*

Le *Trusted Electronic Communications Forum* (TECF) est un consortium du secteur privé sans limites géographiques qui se consacre à la normalisation des technologies et à l'adoption de bonnes pratiques de lutte contre l'hameçonnage, l'usurpation d'identité et le vol d'identité. Il cherche essentiellement à créer, déployer et adopter de manière efficace et efficiente des solutions aux problèmes présentés par des analystes d'études techniques et par ses membres. Des groupes de travail et des comités conçoivent et/ou valident des techniques et des outils qui visent spécifiquement à faire face aux menaces à haut risque décrites par le TECF.

Bibliographie

[b-SMSI-2003] Première phase du SMSI (2003), *Déclaration de principes*.
<http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160>

[b-SMSI-2005] Deuxième phase du SMSI (2005), *Agenda de Tunis pour la société de l'information*.
<http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2266|2267>

[b-APWG] Anti-Phishing Working Group, <http://www.antiphishing.org/>.

[b-IETF RFC 2505] IETF RFC 2505 (1999), *Anti-Spam Recommendations for SMTP MTAs*.
<http://www.ietf.org/rfc/rfc2505.txt>

[b-IETF RFC 2635] IETF RFC 2635 (1999), *DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*).*
<http://www.ietf.org/rfc/rfc2635.txt>

[b-IETF RFC 2821] IETF RFC 2821 (2001), *Simple Mail Transfer Protocol.*
<http://www.ietf.org/rfc/rfc2821.txt>

[b-IETF RFC 2822] IETF RFC 2822 (2001), *Internet Message Format.*
<http://www.ietf.org/rfc/rfc2822.txt>

[b-IETF RFC 3461] IETF RFC 3461 (2003), *Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs).*
<http://www.ietf.org/rfc/rfc3461.txt>

[b-IETF RFC 3685] IETF RFC 3685 (2004), *SIEVE Email Filtering: Spamtest and VirusTest Extensions*.
<http://www.ietf.org/rfc/rfc3685.txt>

[b-IETF RFC 3885] IETF RFC 3885 (2004), *SMTP Service Extension for Message Tracking*.
<http://www.ietf.org/rfc/rfc3885.txt>

[b-IETF RFC 4686] IETF RFC 4686 (2006), Analysis of Threats Motivating DomainKeys Identified Mail (DKIM).
<http://www.ietf.org/rfc/rfc4686.txt>

[b-FTC] United States Federal Trade Commission, *Email Address Harvesting and the Effectiveness of Anti-Spam Filters*, November, 2005.
<http://www.ftc.gov/opa/2005/11/spamharvest.pdf>

[b-Lyris] Lyris Technologies, Inc., *Email Advisor: ISP Email Deliverability Report Card*, 2nd quarter, 2007.
<http://www.lyris.com/resources/reports/deliverability_report_Q22007.pdf>

[b-OECD TF] Groupe de réflexion sur le spam de l'OCDE (2006), *Rapport du groupe de réflexion sur le spam de l'OCDE: Boîte à outils antispams de politiques et mesures recommandées*.
<http://www.oecd.org/dataoecd/63/28/36494147.pdf>

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2009