Petite encyclopédie du courrier électronique et du SPAM

Yves Roumazeilles

(yr@SpamAnti.net)

1. Table des matières

2. Introduction

2.1. Pourquoi cette encyclopédie ?

Tout d'abord, parce que je m'intéresse au courrier électronique et à une forme particulière d'abus de l'e-mail : le SPAM (ou courrier électronique non sollicité). J'ai créé un site web, *SpamAnti* (soit http://www.SpamAnti.net/), où l'on peut retrouver des informations sur le SPAM, les moyens de le combatre, etc.

Mais au-delà des abus, j'ai l'occasion répétée d'aider, de conseiller ou de renseigner des gens de tous horizons au sujet du courrier électronique : des débutants, des gestionnaires de serveurs importants, etc. Cela arrive dans deux types de circonstances : soit mon activité de lutte contre le SPAM, soit – plus prosaïquement – dans mon activité professionnelle de concepteur de site web pour Goélette (http://www.goelette.net/), une société que j'ai créée en 2000.

Je dois répéter certaines informations qui sont souvent difficiles à trouver (en particulier en français). J'ai donc décidé de fournir un document unique qui pourrait être une petite référence et une aide aussi bien pour le débutant attentif que pour l'expert curieux.

2.2. Que contient cette encyclopédie ?

Cette encyclopédie contient beaucoup de choses (certains diront « trop ») :

- Des définitions de termes (certains articles sont très courts et ne comportent qu'une définition minimale ; d'autres comportent des descriptions beaucoup plus étendues. N'y voyez aucune logique sinon celle de mon inspiration et de mes connaissances limitées).
- Des noms et adresses de logiciels contre le SPAM.
- Des noms et adresses de logiciels de messagerie.

Permettez-moi enfin une remarque sur la manière dont j'ai essayé de traiter les informations à caractère historique. Il y a beaucoup de rumeurs et de folklore approximatif sur Internet. Dans le cas des informations à caractère historique en particulier, j'ai essayé de systématiquement citer mes sources afin de permettre une véritable recherche et la confirmation de la qualité des informations dont je dispose. Si vous aviez des raisons de penser que ce que j'ai écrit est inexact, merci de m'indiquer en quoi et sur quelle sources d'information vous vous appuyez (ou à quel titre vous pouvez défendre de vous-même l'information que vous m'apportez).

2.3. Qui en est l'auteur ?

Par endroits dans ce document, vous rencontrerez la première personne du singulier (« Je »). Je suis l'auteur de cette encyclopédie. Si vous rencontrez des erreurs ou voulez des explications, vous aurez peut-être envie de me contacter.

Je peux être joint à l'une des adresses suivantes (le courrier électronique est – vous vous en doutiez – mon moyen de communication de prédilection) :

yr@SpamAnti.net

SpamAnti@roumazeilles.net
roumazeilles@noos.fr
roumazeilles@magic.fr

Afin que les choses soient parfaitement claires, j'insiste sur le fait que ces adresses ne sont pas destinées à recevoir des propositions (commerciales ou non). Toutefois, vous pouvez m'écrire pour des renseignements, de l'aide ou me signaler des erreurs dans cette encyclopédie.

Pour un courrier postal :

Yves Roumazeilles
27-31 rue Robert de Flers
75015 PARIS (FRANCE)

ou (en désespoir de cause) :

Yves Roumazeilles
28 avenue Carnot
64200 BIARRITZ (FRANCE)

D'autres informations complémentaires (y compris une rubrique d'actualité) apparaissent sur mon site web SpamAnti :

http://www.SpamAnti.net/

http://mapage.noos.fr/roumazeilles/spamantf.htm (miroir N°1 en français)

http://perso.magic.fr/roumazeilles/spamantf.htm (miroir N°2 en français)

Je dispose également d'un site personnel. Il ne contient pas d'information particulièrement pertinentes concernant le courrier électronique et le SPAM, mais il peut permettre de prendre contact avec moi (y compris par téléphone) quand toutes les autres solutions ont échoué :

http://www.roumazeilles.net/

http://roumazeilles.cjb.net/

http://mapage.noos.fr/roumazeilles/ (miroir N°1)

http://perso.magic.fr/roumazeilles/ (miroir N°2)

2.4. Remerciements

L'écriture d'un document comme celui-ci a demandé l'aide de nombreuses personnes qu'il serait difficile de remercier individuellement. Mais je veux exprimer ici ma reconnaissance à :

- tous ceux qui essayent de guider mes recherches parfois un peu confuses.
- tous ceux qui font confiance à SpamAnti.net pour l'information à propos du SPAM.
- Manuel Lemos et Christian Lescuyer pour leur apport à l'expression régulière de vérification des adresses de courrier électronique.

- OpenOffice v1.0 qui m'a permis d'écrire ce document sans avoir à recourir à un traitement de textes propriétaire alors que je travaille sur un PC standard. C'est un soulagement important pour moi après des années de dépendance à Microsoft (http://www.openoffice.org/).
- Google et son excellent moteur de recherche sur Internet qui a été une source précieuse et irremplaçable pour vérifier, rechercher, trouver ou corriger cette petite encyclopédie (http://www.google.fr/).

Toutes mes excuses vont à celles ou ceux que j'ai oubliés.

2.5. Informations techniques

Ce document a été rédigé en utilisant Open Office v1.0, suite de logiciels de bureautique du domaine public et librement accessible aussi bien sous Windows que sous GNU/Linux.

Les polices de caractères utilisées sont BakerSignetBT, Souvenir Lt BT et Zurich Cn BT (qui sont librement disponibles pour les utilisateurs de Corel Draw!).

Si vous avez besoin de décrire ce document (par exemple pour nous indiquer où vous avez trouvé une erreur), il est pratique d'indiquer la version (une lettre et un chiffre) qui apparaît à la fin du nom : Encyclopédie B4 (datée du 11 nov 2002).

3. Définitions dans l'ordre alphabétique

Les définitions font le corps de cette encyclopédie. Elles sont groupées par ordre alphabétique (les signes non-alphabétiques apparaissent au début de la liste juste avant la lettre A).

Pour naviguer utilement dans cette liste de définitions, je vous conseille d'utiliser la table des matières (en début de document) qui liste clairement les pages où commencent chacune des lettres de l'alphabet et l'index (en fin de document) qui indique tous les termes utilisés et où ils appraissent utilement (pas uniquement à la page de leur définition).

3.1. @, !, chiffres et autres signes

@ (arobase ou at ou A commercial)

Ce caractère est assurément le symbole le plus évident du courrier électronique. Il est utilisé dans une adresse de courrier électronique pour séparer le nom de l'utilisateur du domaine de l'adresse.

Quelques exemples :

info@SpamAnti.net
SPAM.Anti@roumazeilles.net
Roumazeilles@noos.fr
win95@microsoft.co.uk
Service_Client@ibm.net
adresse-de-test@test.com

De nombreuses prononciations sont rencontrées dans le monde francophone. Il semble que les plus courantes aujourd'hui restent soit « arobase » (le nom du caractère), soit « at » (par référence à la prononciation la plus courante dans le monde anglo-saxon).

! (bang)

Caractère autrefois employé dans les adresses de courrier électronique (principalement avant que ne soient répandu le système DNS de résolution des noms). Il servait à définir un type d'adresse électronique où on indiquait totalement ou presque le chemin physique que devait suivre le message pour parvenir à son destinataire.

Par exemple :

!bigsite!foovax!barbox!me

servait à indiquer un chemin passant par bigsite, puis foovax, puis barbox pour atteindre l'utilisateur me.

La difficulté d'emploi rendait la chose utilisable uniquement par des spécialistes qui avaient une excellente connaissance de l'ensemble de l'architecture du réseau (ce qui n'était envisageable que parce que celui-ci n'avait pas encore atteint les dimensions galactiques de l'Internet d'aujourd'hui).

[...] ou (...)

Une notation couramment employée pour indiquer que l'on a coupé quelque chose. Quand on reprend une partie du texte d'un courrier électronique (dans une réponse à ce courrier), il est considéré comme poli d'indiquer les coupes faites dans le texte original en laissant ce signe à la place de ce qui a été enlevé quand ce n'est pas absolument évident.

>

Il est très courant (même si ce n'est pas obligatoire) d'employer ce caractère pour inclure dans un courrier électronique des portions du courrier auquel on répond.

Par exemple, si je reçois le courrier :

Bonjour,
Je vous invite à la maison dimanche.
Venez sans les enfants.
Pierre

Il sera considéré comme normal de répondre par :

> Je vous invite à la maison dimanche.
Merci pour ton invitation, nous serons là.

> Venez sans les enfants.
C'est entendu. Mais le chien sera avec nous.

Henri et Catherine

On remarquera plusieurs choses. Tout d'abord, les marques > permettent de faire le tri entre ce qui provient du message original et ce qui vient d'être ajouté. Ensuite, elles permettent de mélanger le message original et les réponses ou commentaires.

Enfin, on notera qu'il est possible d'utiliser les marques > sur plusieurs niveaux pour maintenir le contexte complet de la conversation comme dans :

> > Je vous invite à la maison dimanche.
> Merci pour ton invitation, nous serons là.
>
> > Venez sans les enfants.
> C'est entendu. Mais le chien sera avec nous.
>
> Henri et Catherine

C'est parfait pour moi. A dimanche
Pierre

Cette pratique qui provient de l'origine purement textuelle du courrier électronique perd un peu de son aspect sytématique sous la pression de plusieurs facteurs. Certains logiciels rendent cet usage très difficile (c'est le cas d'Outlook Express, par exemple). La pratique du marquage par la couleur rendue possible par l'usage du texte de type HTML permet d'obtenir un fonctionnement proche dans un contexte où les écrans couleur sont courants et où les courriers électroniques ne comportent plus seulement des caractères alphabétiques.

10 (adresses commençant par)

Voir adresses IP privées.

Les 10 spammeurs les plus recherchés par AOL

En mars 1998, Steve Case, le PDG d'AOL, au cœur d'une des premières tempêtes de SPAM, avait dénoncé les « 10 Most Wanted Spammers ». Il est vrai qu'à cette époque le phénomène semblait encore être gérable en s'attaquant seulement à quelques moutons noirs. De nos jours, il est devenu clair que la situation ne sera reprise en main que par la combinaison de plusieurs actions simultanées comme une législation plus ferme, des administrateurs système plus impliqués, des FAIs participant directement à la lutte contre le SPAM et une réelle coopération internationale.

127.0.0 (adresses commençant par)

Ces adresses IP sont des adresses réservées à des fins de test. Par exemple, 127.0.0.1 est l'adresse dite de « localloop » (elle permet toujours de retrouver sa propre machine), ou 127.0.0.2 est l'adresse dite « de test » (elle répond toujours[1]).

169.254.0.0 (adresses commençant par)

Cette famille d'adresses IP (« local link ») ne se rencontre normalement pas dans les en-têtes de courrier électronique parce qu'il s'agit d'un groupe réservé à la configuration automatique dans le cas où une interface réseau ne peut pas se faire attribuer une adresse (par exemple, s'il est impossible de joindre un serveur DHCP). Cette situation donne une adresse (il est souvent difficile de continuer l'exécution des logiciels d'initialisation sans une adresse IP), mais celle-ci est normalement non routable.

192.0.2 (adresses commençant par)

Ces adresses sont réservées à « TEST-NET » pour des besoins de documentation et de test. Elles sont souvent associées à example.com, example.net et example.org dans les documentations (cela évite d'employer des noms et des adresses qui peuvent réellement appartenir à quelqu'un).

172.16 (adresses commençant par)

Voir adresses IP privées.

192.168 (adresses commençant par)

Voir adresses IP privées.

224.0.0 (adresses commençant par)

Ces adresses IP sont des adresses réservées pour les réseaux fonctionnant en mode « multicast » (destinés à la diffusion de divers contenus comme de la musique ou des émissions de télévision). Il est totalement anormal de rencontrer des courriers électroniques qui transitent par des adresses IP comprises entre 224.0.0.0 et 239.255.255.255 (224.0.0.0/4) puisque ces adresses ne sont pas sensées être utilisables pour transporter du courrier électronique (exclusivement en transport de point à point).

7-bit / 8-bit

Le codage de caractères est généralement fait en utilisant le code ASCII (voir l'article correspondant). Toutefois, le code ASCII ne définit formellement qu'un peu moins de 127 caractères (dont les chiffres, les lettres minuscules et majuscules, mais pratiquement aucune lettre accentuée nécessaires en Français

1 En tous cas, elle est censée le faire...

ou dans une autre langue européenne). Ce codage de 127 caractères est réalisable avec 7 bits seulement.

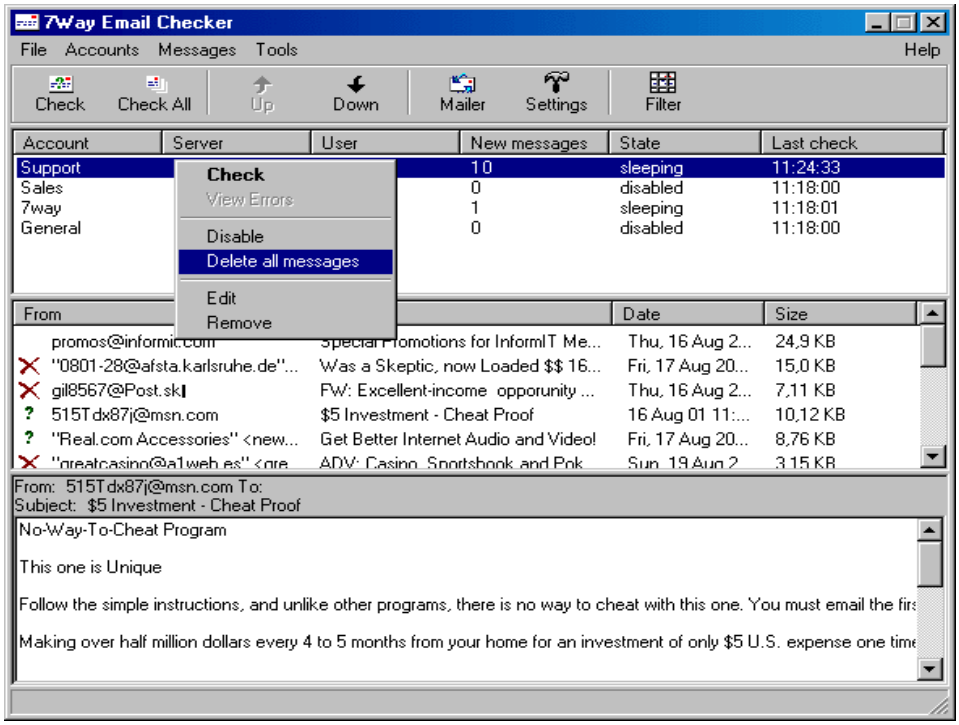
Toutefois, une extension (en réalité, plusieurs extensions, mais nous nous limiterons ici) a été définie pour introduire des caractères accentués. Il s'agit alors d'un codage d'un peu moins de 256 caractères (sur 8 bits).

On parle donc souvent d'ASCII ou d'ASCII 7-bit et d'ASCII 8-bit. Le principal problème étant que le codage 8-bit est parfois encore mal accepté par certaines machines. Par défaut ou par sécurité, les logiciels de messagerie utilisent un codage sur 7 bits, mais permettent de transporter des textes accentués (par exemple, en passant par le format MIME). Mais certains autorisent à utiliser directement un codage sur 8 bits (tout en restant conscient que cela implique certains risques que l'utilisation de MIME aurait permis de contourner).

Je vous conseille d'éviter d'accepter l'option 8-bit de votre logiciel de courrier électronique si vous la rencontrez.

Voir aussi ASCII et Unicode.

7Way Email Checker



Un outil pour Windows de filtrage de courrier électronique de S. Nikitin.

Plus exactement, il s'agit d'un outil qui vous informe de l'arriver de courrier dans votre boîte-à-lettres et qui comporte la capacité de détruire des SPAMs en reconnaissant certains mots-clefs dans l'objet (Subject:) ou dans les en-têtes du courrier électronique alors qu'il reste dans votre boîte-à-lettres.

http://www.start7way.com/

3.2. A

Abréviations

La communication par courrier électronique est souvent une communication très rapide et le rédacteur est tenté d'utiliser des raccourcis dans son expression. Certains acronymes ou abréviations ont acquis le statut de « standard ».

Quelques exemples :

amha : à mon humble avis

a+ : à plus (à plus tard, à bientôt)

mdr : mort de rire

bcp : beaucoup

tlm : tout le monde

Attention : l'emploi de ces raccourcis implique un style relâché qui ne convient pas à tous les courriers électroniques et repose sur le principe partagé d'une compréhension immédiate par toutes les parties impliquées. Comme toutes les formes plus ou moins argotiques, ils ne doivent donc pas faire l'objet d'une utilisation systématique.

On rencontre aussi dans certains cas des raccourcis qui sont d'origine anglaise (quand les interlocuteurs les connaissent).

Quelques exemples :

aka (also known as) : connu sous le nom de, dit aussi, alias

fyi (for your information) : pour ton/votre information

rtfm (Read the f... manual) : lisez la f... documentation

asap (as soon as possible) : le plus tôt possible, aussitôt que possible

Abuse

La plupart des domaines qui se préoccupent de ce que font leurs utilisateurs et de pouvoir traiter leurs « écarts » dans le meilleur délai ont créé un utilisateur particulier : abuse. En génral, il s'agit d'un responsable particulier qui est capable de traiter spécifiquement les plaintes concernant des comportements exagérés ou abusifs des autres utilisateurs (par exemple, pour le domaine domaine.fr, l'utilisateur abuse@domaine.fr traite les plaintes pour comportement abusif des utilisateurs de domaine.fr).

Même s'il s'agit d'un standard couramment respecté, il y a beaucoup de « petits » domaines qui n'ont pas cette adresse particulière et certains autres utilisent une adresse complètement différente.

Par ailleurs, le terme « email abuse » est le terme générique anglais qui recouvre les abus d'emploi du courrier électronique. On le retrouve donc parfois employé sans traduction dans des documents ou des échanges en français.

abuse.net

Un redirecteur de mail (produit par l'infatiguable combattabant du SPAM qu'est John Levine) qui facilite l'identification de l'adresse à laquelle s'adresser pour les cas qui concernent les abus dans un

domaine donné. Il suffit d'écrire à yahoo.com@abuse.net pour que Abuse.net retrouve l'adresse exacte qui doit recevoir ces plaintes.

Recommandé pour ceux qui ne veulent pas passer des heures à chercher ces adresses (surtout pour un administrateur qui risque d'avoir beaucoup de plaintes à présenter). A la première utilisation, il est demandé une confirmation ; mais, ensuite, le fonctionnement est complètement transparent.

http://www.abuse.net/

Acceptable Use Policy (AUP)

Voir AUP.

Acronymes

La communication par courrier électronique est souvent une communication très rapide et le rédacteur est tenté d'utiliser des raccourcis dans son expression. Certains acronymes ou abréviations ont acquis le statut de « standard » et tout le monde les utilise. C'est une habitude courante dans notre société mais particulièrement perceptible dans le monde des technologies.

« Ad hoc IP tools »

Une page web d'outils pour tout faire avec le protocole IP.

http://www.tatumweb.com/iptools.htm

Address munging

Il s'agit de l'action de modifier une adresse de courrier électronique afin de s'assurer qu'un message ne peut être envoyé qu'à la condition que l'adresse soit modifiée (manuellement).

Le principe repose sur le fait qu'une modification mineure et compréhensible par un être humain sera virtuellement impossible à reconnaître par un programme automatique de SPAM. Par exemple, si mon adresse apparaît comme Yves_PAS_DE_SPAM_ICI@PAS_DE_SPAM_ICI_Roumazeilles.net et que je précise à mes correspondants qu'il faut enlever « PAS_DE_SPAM_ICI » de l'adresse, un robot collecteur d'adresse s'y trompera mais la plupart des êtres humains sauront retrouver l'adresse véritable Yves@Roumazeilles.net et l'utiliser pour m'envoyer du courrier électronique.

Cette approche est souvent employée par des utilisateurs de services très générateurs de SPAM. Par exemple, sur les forums Usenet, il est confortable de donner son adresse de courrier électronique aux lecteurs, mais de nombreux robots de spammeurs en profitent pour l'enregistrer. On peut ainsi se prémunir contre les risques de collecte automatique de son adresse.

Les limitations sont tout de même significatives :

1. la modification à opérer peut vous paraître claire mais ce n'est pas forcément exact en ce qui concerne votre correspondant (en particulier, si vous ne parlez pas - ou pas bien - la même langue). Cela mènera à des essais, des échecs, et peut-être à l'abandon pur et simple de la part de votre correspondant.
2. c'est désagréable pour vos correspondants qui ne peuvent plus se contenter de recopier votre adresse ou de cliquer sur le lien qui leur est indiqué. Il faut faire une modification en plus. Cet inconfort est parfois peu conciliable avec votre activité première (par exemple, si vous êtes ingénieur commercial d'une entreprise, il est difficilement possible d'imposer cela à tous vos correspondants).
3. c'est trop compliqué pour certains types de communications (par exemple, une annonce de presse en entreprise).

4. C'est contraire à la plupart des RFC concernant la gestion du courrier électronique (cela implique que l'adresse que vous « publiez » peut être mal comprise par des programmes « utiles »).

Toutefois, comme il est pratiquement impossible à un programme automatique de reconnaître ce qu'il faut faire comme modification, la solution a un avantage indéniable.

Au delà des ajouts de texte dans l'adresse de courrier électronique (décrits ci-dessus), on rencontre d'innombrables autres cas possibles (l'imagination est libre) comme :

- inverser des lettres : sevY@selliezamuoR.net,
- décrire le processus de construction de l'adresse : « Prénom@Nom.net ».

Enfin, il est souvent utile de noter que le nom de domaine que vous « créez » dans ce processus ne doit pas exister. Imaginez les conséquences, si votre courrier électronique était adressé à quelqu'un d'autre que vous parce que vous avez choisi une méthode de « munging » trop simple (si on l'inverse, aol.com donne loa.com, un nom de domaine qui existe bel bien).

Tous ces mécanismes sont plus ou moins souples et efficaces, bien sûr. A chacun de choisir.

Address Munging FAQ (la foire aux questions sur l'address munging) :

Spam-Blocking Your Email Address
http://members.aol.com/emailfaq/mungfaq.html

Note du « traducteur »: mung (Mash Until No Good, d'après le Jargon File ; soit en français « écraser jusqu'à le rendre inutile ») est un mot d'argot ou de jargon qui se prête donc mal à la traduction. J'ai donc tout simplement renoncé à en produire une traduction personnelle alors que je ne connais pas de terme francophone employé pour décrire cette opération. Prévenez-moi si vous connaissez un équivalent français. Merci d'avance.

Adresse

L'adresse d'un utilisateur de courrier électronique joue exactement le même rôle que dans le cas d'un courrier postal : elle permet au préposé au transport du courrier de déterminer où l'envoyer.

Le caractère @ est utilisé dans une adresse de courrier électronique pour séparer le nom de l'utilisateur du domaine de l'adresse :

Quelques exemples :

info@SpamAnti.net
postmaster@aol.com

La partie à droite de l'@ (dans nos exemples, USA.net ou aol.com) indique le fournisseur de messagerie (celui qui fournit la boîte-à-lettres). Techniquement, on l'appelle le nom de domaine. La partie à gauche de l'@ (dans nos exemples, info ou postmaster) donne le nom de cette boîte-à-lettres, autrement appelé le nom d'utilisateur.

Les logiciels utilisent ces informations pour désigner de manière non équivoque un utilisateur de courrier.

Une notation utile à retenir par ceux dont le logiciel de messagerie électronique ne facilite pas le nommage des adresses de courrier électronique, est celle qui combine un nom sous une forme libre et une adresse technique (souvent dite sous forme canonique) :

"Nom" <utilisateur@domaine.fr>

Entre les guillemets, on peut mettre un nom descriptif (éventuellement avec des espaces et des lettres accentuées) ; entre les crochets apparaît une adresse traditionelle. Exemple :

"Yves Roumazeilles à SPAM.Anti!" <info@SpamAnti.net>

NOTE : contrairement à une croyance très répandue en France, le respect des majuscules ou minuscules n'est pas nécessaire dans une adresse de courrier électronique sur Internet. Toutefois, une adresse de courrier électronique utilisant une technologie non Internet peut apporter cette contrainte (mais cela reste rare). Ainsi, info@SpamAnti.net et INFO@spamanti.net désignent exactement la même adresse et il n'y a pas de système de messagerie Internet qui soit sensible à cette différence.

Adresse bidon, adresse contrefaite

En anglais, « bogus address » et « forged address ».

Il est important de noter que de nombreux spammeurs utilisent des adresses bidons dans leurs mails. C'est un des moyens les plus courants de détourner l'attention de l'origine véritable des SPAMs. Le plus souvent, il s'agit d'une adresse complètement inventée. Parfois, il s'agit de l'adresse de quelqu'un d'autre (sans relation avec le SPAM). Plus rarement, mais cela arrive, il s'agit de l'adresse de quelqu'un qui combat le SPAM.

Adresse IP

L'ensemble des machines présentes sur Internet sont identifiées par un numéro qui lui permet de communiquer avec les autres machines du réseau. On retiendra que les adresses IP sont gérées par un standard intitulé IPv4 (Internet Protocol version 4) et que ce standard est en cours d'évolution (pour pouvoir accueillir considérablement plus de machines qu'aujourd'hui) sous le nom d'IPv6 (Internet Protocol version 6).

En IPv4, une adresse IP est un nombre à 32 bits, généralement représenté sous forme d'un groupe de 4 chiffres décimaux séparés par des points, comme dans les exemples suivants :

112.120.1.15
10.0.0.1
137.240.5.39

D'autres notations sont parfois reconnues mais sont beaucoup moins courantes que la notation pointée indiquée ici. Toutefois, les spammeurs utilisent souvent ces autres notations pour rendre plus difficile la tâche de leurs adversaires. On trouve notamment une notation binaire (uniquement constituée de 0 et de 1), et une notation décimale pure (un nombre « classique » mais souvent très grand).

Special-Use IPv4 Addresses (adresses IPv4 à usage spécial)
http://www.ietf.org/internet-drafts/draft-iana-special-ipv4-05.txt

Adresses IP privées

L'Internet Assigned Numbers Authority (IANA) a réservé les trois blocs suivants d'adresses IP comme espace d'adressage pour des Internet privés (ou des sous-réseaux privés).

10.0.0.0	-	10.255.255.255 (préfixe 10/8)
172.16.0.0	-	172.31.255.255 (préfixe 172.16/12)
192.168.0.0	-	192.168.255.255 (préfixe 192.168/16)

Les personnes qui cherchent à déterminer l'origine d'un mail (d'un SPAM par exemple) rencontrent souvent des adresses de ce type à cause d'erreurs de configuration de certains serveurs (parfois volontaires de la part d'un spammeur). En général, cela indique une machine dont l'identification va être plus difficile que si elle se contentait de publier son adresse IP « officielle ».

Adresses jetables

Une approche pour contrôler le SPAM consiste à utiliser une adresse de courrier électronique « jetable » pour chaque formulaire que vous remplissez. Si ces adresses sont correctement gérées (et certains services Internet vous le proposent), il s'agit alors d'un contrat entre un site et vous pour utiliser une adresse et une seule. Vous acceptez de recevoir du mail de ce site uniquement sur cette adresse. Cela évite les conséquences de la revente de votre adresse (cette adresse jetable) à un spammeur.

Voir Sneakemail ou MailExpire.

ADSL

Asymetric Digital Subscriber Line.

Une technologie haut-débit qui permet de connecter un utilisateur à son Fournisseur d'Accès Internet tout en se contentant de la ligne téléphonique existante (contrairement au cable qui demande la pose d'un cable particulier). Il s'agit certainement de la technologie haut-débit à destination du grand public qui connaît actuellement la plus forte progression dans les pays occidentaux.

Elle s'accompagne aussi couramment d'une offre de connexion illimitée à Internet qui offre plusieurs solutions à des problèmes comme la possibilité d'avoir une adresse IP fixe (pour installer un serveur par exemple). Cela a déjà eu plusieurs conséquences sur l'emploi du courrier électronique, dont :

- multiplication du nombre de serveurs de messagerie
- existence de nombreux serveurs de messagerie mal configurés (voir l'article sur les « open relays »)
- apparition de serveurs qui ne disposent pas réellement d'un administrateur (ou d'un administrateur ni compétent, ni conscient des enjeux de sécurité)

Par certains aspects, tout cela a facilité l'extension du phénomène du SPAM dans les années récentes. Ce n'est pas une bonne raison pour condamner l'ADSL (ou le haut-débit) mais pour exiger plus d'attention, de soin et une meilleure qualité de la prestation globale de sécurité des Fournisseurs d'Accès Internet, des vendeurs de logiciels (en particulier Microsoft). Et, cela demande à former les utilisateurs à la sécurité (les utilisateurs de cartes bancaires à puce sont bien invités fermement à ne jamais divulger leur code confidentiel).

Finalement, cela est en train de permettre le développement d'un marché pour les outils de sécurité à l'intention du grand public.

Alerte par courrier électronique

Certains services existent qui permettent d'être alerté de différents événements par l'intermédiaire d'un courrier électronique. Ces services sont souvent proposés sur un site web. On retrouve aussi bien des alertes liées au franchissement de seuils de prix (sur des sites boursiers, des sites de ventes aux enchères, des sites de négociations de prix, etc.) que des messages fournissant des nouvelles fraiches (dans le domaine d'un sport par exemple). Ces services sont souvent appréciés du fait de leur quasi-instantanéïté associée à une intrusion très limitée.

Alias out

Verbe anglais jargonnant qui décrit l'action de se débarrasser de quelque chose en lui donnant un autre nom. Voir l'article sur le fichier hosts pour une description de la technique dite d'out aliasing qui emploie ce fichier.

Also-Control:

En-tête normalement réservé aux messages Usenet (ne devrait pas apparaître dans les en-têtes de messages de courrier électronique).

alt.religion.scientology

Groupe de discussion Usenet qui est - historiquement - le plus souvent attaqué par des SPAMs (au sens des abus de groupes de discussion Usenet et non des abus du courrier électronique). Il traite de l'Eglise de Scientologie (une secte, au sens du rapport parlementaire français sur les sectes, créée par l'ancien écrivain de Science Fiction Ron Hubbard) et on y retrouve de farouches affrontements verbaux et techniques entre membres de la secte et opposants actifs.

Alternate-Recipient:

Détermine si le message peut être transmis à un « alternate recipient » (un destinataire de remplacement) si la transmission au destinataire normal échoue.

Exemple :

Alternate-Recipient: Allowed

America On Line

Voir AOL.

Annuaires d'adresses de courrier électronique

On a souvent envie de disposer d'un annuaire (semblable à l'annuaire téléphonique) pour les adresses de courrier électronique. Certains sites présentent un tel service. En voici une liste partielle (ils sont tous en anglais) :

Nom du service	*Remarques*
WhoWhere	http://www.whowhere.com/
Yahoo! People search	http://people.yahoo.com/
World Email Directory	http://www.worldemail.com/
Bigfoot	http://www.bigfoot.com/
Switchboard	http://www.switchboard.com/
Infospace	http://www.infospace.com/
IAF	http://www.iaf.net/

Toutefois, on notera qu'on ne peut pas considérer ces services comme très fiables. Les résultats sont très inégaux (et le plus souvent nuls) selon la personne que vous recherchez. L'organisation très décentralisée (et peu coordonnée) d'Internet interdit pratiquement un tel service. Les sites web qui le proposent essayent de trouver tous les endroits où apparaissent des adresses identifiables, mais ils ne

peuvent obtenir que des résultats partiels à cause de l'absence de déclaration (hormi une inscription volontaire). Souvent, on ne trouve pas la personne recherchée, on trouve un homonyme (la localisation géographique est très rare dans ces annuaires), ou une adresse périmée.

On notera que la plupart de ces sites utilisent des robots qui balayent Internet à la recherche d'adresses de courrier électronique. Ils ne sont *a priori* pas à l'origine de SPAM, même s'il est parfois arrivé qu'ils soient détournés de leur objectif initial. Mais ces abus semblent ne plus se rencontrer aujourd'hui[2].

Une des méthodes qui permettent de retrouver l'adresse de courrier électronique de quelqu'un que vous connaissez (et qui marche aussi bien que ces services) consiste à entrer le nom de la personne recherchée dans un moteur de recherche du web comme Google (http://www.google.fr/) ce qui vous dirigera sur une ou plusieurs pages où cette personne est citée. Avec un peu de chance, son adresse de courrier électronique se trouvera sur l'une de ces pages (peut-être sa page personnelle).

Une autre qui n'est valable qu'en France consiste à consulter les pages jaunes ou les pages blanches de France Telecom (http://www.pagesblanches.fr/) où l'on peut trouver les adresses de courrier électronique de ceux et celles qui ont décidé de les publier volontairement par ce moyen. Toutefois, elles ne sont certainement pas publiées en vue d'une utilisation publicitaire et spammer ces adresses serait un comportement clairement répréhensible.

Anomy

Un outil de nettoyage/filtrage des messages électroniques pour Linux/Unix.

http://www.anomy.net/

Anonymizer

Service qui permet de rendre anonyme une navigation ou un courrier électronique. Il existe (ou a existé) de nombreux serveurs qui proposent ce genre de service. Mais la légalité d'un tel service reste très sujette à caution dans la plupart des pays disposant d'une législation sur les communications. La plupart de ces services ont donc soit une durée de vie assez réduite, soit des limitations importantes pour éviter de pouvoir être détournés de leur objet initial (de protection de la vie privée en dissimulation d'activité illégale).

Anonymous remailer

Ce service permet d'envoyer un e-mail qui a toutes les caractéristiques de l'anonymat. Pour l'essentiel, le remailer est un type de MTA qui efface toutes les informations initialement contenues dans les en-têtes et qui les remplace par sa propre information, dissimulant ainsi l'origine du courrier électronique.

Il existe un certain nombre de ces services. Dans la plupart des cas, ils sont situés dans des pays où la législation est suffisamment flexible pour que le propriétaire du service ne soit pas trop rapidement mis en cause quand un utilisateur l'exploite pour des activités illégales. Dans de nombreux cas, l'anonymat peut être rompu par les autorités locales dans certaines conditions.

La plupart de ces services font leur possible pour éviter d'être « abusés » et, en particulier, ne tolèrent pas les envois en nombre.

2 Les fournisseurs de ces services sont devenus très sensibles à la possibilité d'être détournés de leur objectif initial et prennent des mesures actives comme de ne jamais afficher les adresses dans l'annuaire lui-même (ils proposent au contraire un formulaire web par lequel on peut envoyer un court message à la personne que l'on pense avoir trouvé).

AOL (America On Line)

Le plus gros fournisseur d'accès Internet mondial, AOL utilise aussi un nombre important de protocoles complètement propriétaires. Pour cette raison, les courriers électroniques provenant de (ou à destination de) AOL peuvent rencontrer des problèmes spécifiques qui demandent une expérience particulière de la part des administrateurs de serveurs de courrier électronique.

On notera également que (à tort ou à raison) les utilisateurs d'AOL ont une très mauvaise réputation sur Internet en général : celle d'être stupide au delà de tout espoir de sauvetage. Cela vient probablement des méthodes de recrutement-client d'AOL qui cible le grand public par l'intermédiaire des utilisateurs les moins expérimentés.

Pour avoir une idée (en anglais) du genre d'opinion qui peut être exprimée, on pourra visiter la page *satirique* de Something Awful :

http://www.somethingawful.com/nointelligence/index.htm

Cette réputation est importante parce que l'on rencontre encore (même si c'est devenu rare) des domaines qui refusent tout simplement tout courrier électronique provenant d'un client AOL. La plupart des clients habituels d'AOL n'en soufriront sans doute pas (il s'agit surtout de communautés très militantes et souvent technophiles qui ne ressemblent guère au public moyen d'AOL).

Toutefois, dans l'espoir de participer à la régulation de la pratique du SPAM, AOL propose à ses abonnés un service intitulé « Marketing preferences ». Il permet de choisir de ne recevoir que certaines offres (ou aucune). Cette possibilité revient régulièrement sur le devant de la scène pour ses faiblesses, la nécessité de renouveler régulièrement l'expression de la volonté de ne plus rien recevoir, son impossibilité à réellement arrêter le SPAM malgré ce qui est impliqué dans la présentation qui en est faite le plus souvent.

AOL a eu la réputation d'avoir des services internes très difficiles à joindre (en particulier, pendant longtemps il a été presqu'impossible de trouver un contact valable pour transmettre une plainte pour abus par un des utilisateurs d'AOL). Cette réputation n'est toujours pas effacée, mais il est maintenant possible de les contacter par l'intermédiaire des contacts suivants :

Service	*Adresse*
Traitement des abus par les clients AOL	abuse@aol.com
Gestion (interne) des problèmes techniques des clients AOL	support@aol.com

API-PL

Observatoire national des professions libérales (en France), l'API-PL (ou Association pour la Promotion d'Internet – Professions Libérales) a émis plusieurs rapports utiles à cette catégorie d'internautes un peu à cheval entre utilisateur à titre personnel et à titre professionnel. En juillet 2002, l'API-PL a même produit et publié un ensemble riche de plus de 100 conseils pratiques pour les internautes.

http://www.apipl.org/guideantispam.html

Apparently-To:

Des messages avec de nombruex destinataires ont parfois une longue liste d'en-têtes de la forme « Apparently-To: info@SpamAnti.net » (une ligne par destinataire). Ces en-têtes ont longtemps été considérés comme peu courants dans le cas d'un courrier électronique traditionnel, mais comme une

marque de fabrique des listes de messagerie. Les logiciels récents de gestion de liste de messagerie ont maintenant appris à ne plus recourrir à cette longue liste d'en-têtes.

Cet en-tête n'est pas standard et n'est normalement utilisé que par Sendmail quand il ne trouve aucun en-tête `To:` mais peut déterminer une destination à partir de « l'enveloppe » du message (à partir des échanges de données du protocole SMTP).

Ce comportement est considéré comme non-souhaitable parce qu'il peut mener à divulguer certains destinataires qui devaient rester cachés dans une ligne `Bcc:` et parce que les MTAs se doivent de ne pas modifier les en-têtes autrement que par l'ajout d'en-têtes `Received:`.

Appels

On reçoit souvent pas Internet (et principalement par courrier électronique) des appels en tous genres qui nous invitent à participer activement à tel ou telle activité, à supporter tel ou tel groupe ou personne. Toujours en y donnant la plus grande publicité possible (« transmettez ce message à tous vos amis »).

De manière générale, il convient de toujours **vérifier** l'origine et le contenu du message. On ne compte plus les appels à assistance pour des enfants malheureux qui n'ont jamais existé, pour des populations sinistrées qui ne sont même pas au courant de leur « malheur », etc. Nombre de ces messages sont soit erronés, soit tout simplement mensongers.

En les propageant, vous ne vous contentez pas de participer au phénomène de *légende urbaine*, mais vous vous discréditez à bon compte auprès de vos amis/relations/contacts. On peut se tromper, mais le fait de ne pas être le premier (ni le dernier, d'ailleurs) ne vous protège pas.

Les appels sont de plusieurs ordres, mais les plus courants peuvent se regrouper dans un petit nombre de catégories :

- Les annonces de virus : ils sont généralement les plus terribles jamais rencontrés, ils ont été détectés par des instances de confiance (Microsoft, IBM, le gouvernement, un fabricant d'anti-virus, etc.) ; et, dans 99,99% des cas, il ne s'agit que d'un canular[3].
- Les appels à la générosité : entre Craig Shergold, petit garçon atteint d'une tumeur au cerveau et maintenant guéri depuis longtemps, qui n'espère plus avoir jamais sa boîte-à-lettres vide et les Brians ou autres prétendus enfants malheureux, on s'y perd dans les demandes d'aide. Le Livre Guinness des records a fini par refuser d'enregistrer les records liés à ce genre de situation pour éviter de propager ces exagérations invraisemblables.
- Les pyramides ou scams : là il s'agit d'escroqueries pures et simples. Les lettres-chaînes sont purement et simplement interdites dans de nombreux pays dont les Etats-Unis et la Belgique (pas la France, à ma connaissance). En Belgique, on peut même porter la chose à la connaissance de la CCU (Computer Crime Unit) de la PJ (Police Judiciaire) (site web : http://www.gpj.be/).

Tous ces messages ne sont pas des plaisanteries, des escroqueries ou des canulars. Mais il convient de **vérifier** avant de s'y conformer. Dans l'immense majorité des cas, on passera son chemin. Dans quelques cas, après vérification, vous serez tenté de faire facilement une bonne action.

3 A ce jour, je n'en ai encore reçu AUCUN qui soit une alerte sérieuse. Quand bien même cela arriverait, un anti-virus à jour vaut mieux que les conseils affolés qui sont propagés.

Approved:

Réservé à des messages Usenet qui ont été approuvés par un modérateur de groupe de discussion pour distribution à l'intérieur d'un groupe modéré (un groupe de discussion dont le trafic est contrôlé et validé par un ou plusieurs modérateurs).

Argentine (2000-2001)

Ce pays est devenu (en 2000 et 2001, donc avant les considérables problèmes économiques de 2002) un des plus gros producteurs de SPAM. Pour des raisons qui ne sont pas claires pour moi, de nombreux SPAMs hispanophones ont commencé à envahir les boîtes-à-lettres du monde entier en provenance d'Argentine. Cela démontre à l'envie comment il est préferrable (pour un spammeur) de cibler le plus grand nombre possible de destinataires plutôt que d'essayer de faire un tri (les seuls hispanophones dans le cas présent) qui pourrait faire perdre un « client potentiel ».

A ce sujet, les hispanophones visiteront avec intérêt le site de AntiSpam Argentina (le premier site local de lutte contre le courrier électronique abusif) :

http://www.antispam-argentina.8m.net/

Edmundo Valenti, président du chapître argentin de l'ISOC a été entendu disant sur Wired : « En Argentine, la pratique du SPAM n'est pas vraiment considérée pour ce qu'elle est - une violation des droits personnels de chacun. De nombreuses entreprises tout à fait sérieuses ici ne pense pas pratiquer le SPAM quand elles produisent des déluges de publicité par courrier électronique ».

Note : l'Argentine est aussi un pays où en Novembre 2001 a été proposé une loi qui rendrait le courrier électronique complètement privé (même dans une entreprise) avec une garantie Constitutionnelle. Toutefois, il s'agit aussi d'un pays où les hackers sont difficiles à poursuivre en l'absence d'une loi spécifique comme l'indique un jugement rendu dans ce sens le 16-avril 2002 (à ce sujet, voir les articles http://www.theregister.co.uk/content/6/24877.html et http://uk.news.yahoo.com/020415/80/cwsso.html).

Le vrai et le faux sur la loi anti-SPAM en Argentine (en espagnol) :

http://www.rompecadenas.com.ar/leyspam.htm

Arobase

Le linguiste Berthold Louis Ullman, à qui l'on doit cette hypothèse, date son apparition au VIe siècle (au Moyen-Âge, donc), où des moines copistes l'ont utilisé comme raccourci deu mot latin « ad » qui a des significations variées qui vont de « à » à « auprès de » en passant par « vers » (la copie manuelle des ouvrages a forcé à l'apparition de certaines notations abrégées dont l'esperluète (&) qui tenait la place de la conjonction latine « et »).

Le mot arobase serait, quant à lui, la déformation de a rond bas (de casse), c'est à dire a minuscule entouré d'un rond. Mais il y a confusion avec une unité de mesure espagnole l'arroba (25 livres espagnoles, soit 11,502 kg) dont le nom français est arrobe. Cette mesure espagnole viendrait elle-même de l'arabe ar-roub (le quart).

Quoi qu'il en soit, le nom français préconisé par la Délégation Générale à la Langue Française pour ce caractère est le terme arrobe. Le monde universitaire et informatique à l'origine de son expansion mondiale parle plus volontiers d'arobase, terme qui, en français, semble le plus employé.

On a aussi vu utiliser le même signe @ dans le commerce pour indiquer « à » dans le prix par unité d'un produit (comme dans « 12 œufs @ 0.10 € = 1.20 € »). Même si l'époque est moins clairement connue pour cet usage, cela explique sans doute la présence du signe sur les claviers de machines à écrire dès le dix-neuvième siècle, puis sur ceux des ordinateurs du vingtième siècle.

Visiter http://www.herodios.com/herron_tc/atsign.html pour une liste étonnament exhaustive de noms dans différentes langues (rédigé en anglais).

ASCII

American Standard Code for Information Interchange

ASCII (prononcer « aski ») est le le standard développé par par l'American National Standards Institute (ANSI X3.110-1983) pour décrire comment les ordinateurs écrivent et lisent les caractères. La plupart des « fichiers texte » sont – en fait – au format ASCII.

Le code ASCII décrit 127 caractères, incluant lettres, chiffres, signes de ponctuation et certains caractères de contrôle (comme le code de la fin d'une ligne). Chaque lettre ou caractère est représenté par un nombre : le A majuscule est le numéro 65 et le chiffre 0 est le numéro 48.

Aujourd'hui, la grande majorité des systèmes informatiques utilisent le code ASCII standard ou un de ses dérivés. En effet, d'une part les anciens « concurrents » d'ASCII (comme EBCDIC d'IBM ont a peu près disparu), d'autre part les codes permettant de représenter d'autres caractères (par exemple les lettres accentuées) sont quasiment tous aujourd'hui basés sur ASCII et sont compatibles avec le code ASCII.

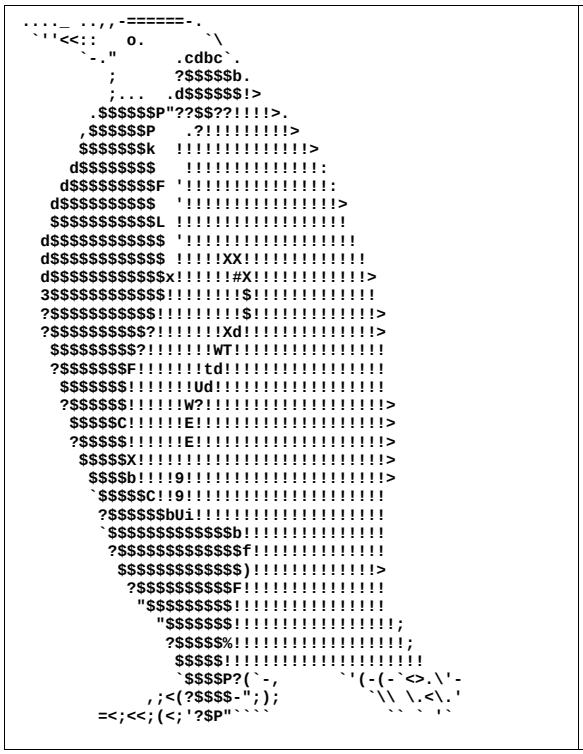
Voir aussi binaire.

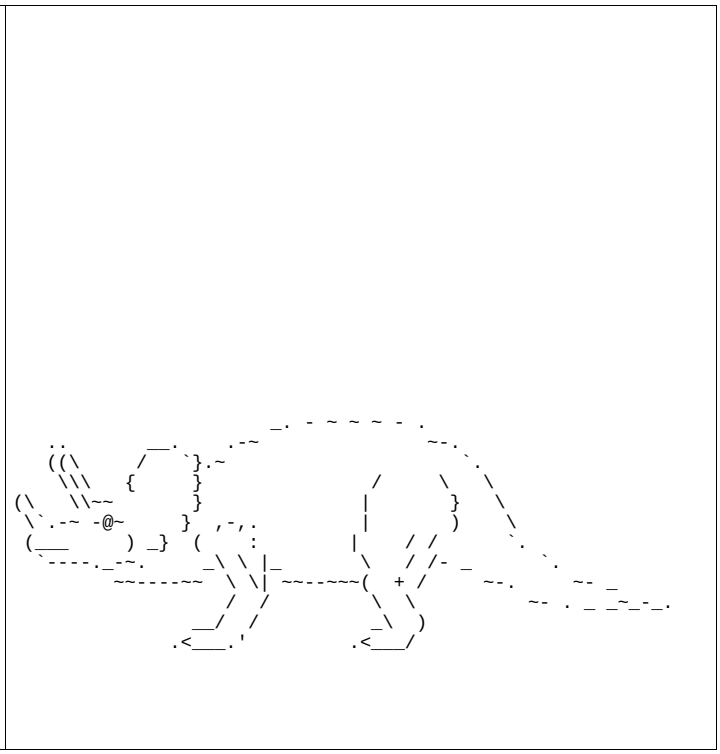
ASCII art

Le terme désigne un forme d'art graphique qui n'utilise que des caractères pour représenter un dessin ou une image. Depuis que les fichiers attachés et les pièces jointes sont facilement accessibles aux rédacteurs de courrier électronique, et que les connexions ont gagné en vitesse, ce mode d'expression a perdu beaucoup de sa valeur et reste totalement ignoré d'un certain nombre d'utilisateurs d'Internet.

L'ASCII art a surtout été utilisé dans les signatures des courriers électroniques qui ont accueilli librement cette forme d'expression même lorsqu'elle a pris des proportions peu compatibles avec la Netiquette (voir les exemples ci-dessous).

Le groupe de discussion Usenet alt.ascii-art regroupe un certain nombre d'amateurs et voit passer un certain nombre d'exemples.





On remarquera facilement que pour pouvoir être affichés correctement ces dessins exigent d'utiliser une police ou une fonte non-proportionnelle (dont tous les caractères ont la même largeur) comme Courrier ou Courier New.

Attachement

Ce terme anglais (ou franglais) est parfois employé sous une prononciation française. Voir « fichier attachés ».

Attaque DoS

Voir aussi Denial of Service (DoS).

AUP

Acceptable Use Policy (en français « règles d'usage acceptable »).

Ensemble de règles qui décrit les conditions d'usage qui sont considérées comme « acceptables » par un Fournisseur d'Accès Internet. Ces règles sont communiquées par le FAI à ses clients lors de leur inscription. Dans la grande majorité des cas, elles excluent tout comportement abusif. Leur rédaction est entièrement laissée à l'appréciation du FAI (parfois, on trouve des sanctions financières dans le cas d'envoi de SPAM).

Une exemple d'AUP conforme aux contraintes légales européennes peut être trouvé chez UUnet Belgique :

http://village.uunet.be/ENG/Infodesk/html/Info_aup.html

Authenticated sender

On rencontre parfois (en 2002, cela commence à être moins courant) dans certains courriers électroniques l'en-tête suivant :

Comments: Authenticated sender is [un nom ou une adresse]

Il s'agit d'un en-tête très spécifique à de très vieilles versions de Pegasus mail. À une époque où ce logiciel gratuit pouvait encore être utilisé pour envoyer du courrier électronique en masse. Il peut être utilisé comme un marqueur très sûr pour reconnaître un courrier électronique comme étant du SPAM, étant donné qu'il ne semble plus utilisé à d'autres fins que le SPAM.

Exemple :

Comments: Authenticated sender is john.doe@best.isp.net

Authentification

Il s'agit du processus qui permet à un utilisateur (ou plus rarement, à une machine) de se faire reconnaître de manière certaine par une machine. Le processus d'authentification peut utiliser de nombreux procédés parfois très complexes, mais le plus courant consiste à demander un nom d'utilisateur et un mot de passe (seul l'utilisateur lui-même est censé connaître le mot de passe).

Auto-answer

Voir réponse automatique.

3.3. B

Backbone

La structure de réseau à très haute vitesse qui relie les plus importants serveurs d'Internet. Par nature, cette partie d'Internet est changeante et mal connue de la plupart des utilisateurs qui savent pourtant qu'il existe une telle charpente pour soutenir le réseau des réseaux. Le terme est parfois utilisé de manière très lêche pour décrire n'importe quelle connexion à haute vitesse entre deux serveurs ou deux routeurs importants du réseau.

Une traduction approximative pourrait être « épine dorsale ».

Bande passante

Terme employé de manière assez imprécise et qui désigne généralement la capacité à transporter des informations sur un lien de communication. On parle de la bande passante d'un Fournisseur d'Accès Internet (ou FAI) pour décrire la capacité de transport de données de son lien vers Internet (généralement mesurée en méga-octets par seconde). On emploie aussi parfois le terme de débit théorique ou de débit théorique maximum.

Bang

La prononciation la plus courante du point d'exclamation (!).

Bcc:

Un des en-têtes les plus « basique » du courrier électronique, le champ Bcc: (comme le champ Cc:) désigne une liste de destinataires secondaires du message qui doivent en recevoir une copie mais qui

ne doivent pas être visibles dans le message lui-même (Bcc: signifie littéralement *Blind Carbon Copy* ou *Copie carbone aveugle* ou *Copie carbone invisible*).

On peut inscrire plusieurs adresses de courrier électronique sur la ligne Bcc: en les séparant par une virgule.

Exemple :

Bcc: info@SpamAnti.net, John.Doe@stop.abuse.net

Voir aussi Cc:

Binaire

Se dit d'un fichier ou de tout autre groupe d'information qui ne peut pas être représenté par les seuls caractères ASCII humainement lisibles. Plus souvent encore, se dit d'un programme exécutable.

Dans tous les cas, l'adjectif est à rapprocher des fichiers attachés et des pièces jointes qui ont été *inventés* pour permettre le transport de fichiers binaires (non uniquement de texte).

Voir aussi ASCII.

BIND

Berkeley Internet Name Daemon. Une des implémentations les plus courantes du protocole DNS.

BinHex

BINary HEXadecimal

Afin de faciliter le transport de fichiers binaires, il est souhaitable de les « convertir » en ASCII. BinHex est une méthode couramment employée chez les utilisateurs de Mac. Le format MIME – plus standard – remplace peu à peu celle-ci.

Black list

Voir liste noire.

BlackHole

Un outil bien utile pour les Fournisseurs d'Accés Internet pour lutter contre le SPAM. BlackHole s'installe sur les serveurs, filtre les relays ouverts (compatible avec la plupart des RBL), filtre les virus, contrôle les en-têtes de courriers électroniques, etc.

http://the.groovy.org/blackhole.shtml

Body

Voir corps.

Bombardeo publicitario

SPAM en espagnol. Littéralement « bombardement publicitaire ».

Bombe

Certains messages de courrier électronique sont dénommés « bombes » quand ils contiennent (ou quand on pense qu'ils peuvent contenir) un élément susceptible de détruire ou détériorer l'ordinateur de

celui qui le reçoit. Cette dénomination reste toutefois moins utilisée en France que son équivalent anglais (« email bomb ») aux USA ou au Royaume Uni.

Boucle

Voir « loop ».

Bounce

Dans le contexte d'un logiciel de messagerie électronique, action qui consiste à transférer un message reçu (très proche de l'action forward), mais sans rien y ajouter. Dans la plupart des cas, le message semble venir de l'expéditeur original même s'il a transité par la machine et le logiciel de messagerie électronique d'un intermédiaire.

Cette fonction n'est pas toujours présente sur les logiciels de messagerie électronique d'entrée de gamme.

Bourse

La Bourse est un endroit où certains pensent pouvoir faire de l'argent facilement (et certains y parviennent, parfois en utilisant le SPAM comme dans quelques pratiques de « pump and dump[4] »).

Si vous détectez une fraude à la Bourse sur une place américaine (par exemple, le NYSE ou une de ses structures comme le NASDAQ), adressez tous les éléments dont vous disposez à enforcement@sec.gov (la SEC ou Securities and Exchange Commission est l'équivalent de la Commission des Opérations de Bourse ou COB ou « gendarme » de la Bourse de Paris). Non seulement, ils vont en tenir compte, mais ils engagent régulièrement des poursuites et collent en prison un certain nombre de contrevenants (il est illégal de propager des rumeurs dans le but de faire bouger les cours d'une ou plusieurs valeurs, même si vous n'en profitez pas vous-même).

Note personnelle : à ma connaissance, il n'y a pas d'adresse e-mail équivalente à la Bourse de Paris ou à la Bourse de Bruxelles). Mais si vous trouvez ça, j'aimerais la connaître.

Bozo (ou filtre à Bozo ou liste de Bozos)

Programme qui permet de filtrer le courrier électronique en retirant les messages provenant de certains utilisateurs considérés comme indésirables (les Bozos).

Le terme semble venir de Bozo le clown, personnage d'une série télé pour enfants des années 70-80.

Brightmail

Brightmail Inc. fournit une solution de filtrage du courrier électronique. La solution est particulièrement bien adaptée à un usage par un Fournisseur d'Accès Internet.

http://www.brightmail.com/

Bulk email

Courrier électronique en masse.

La définition technique donnée par la FAQ [4] est : plus de 25 destinataires en une seule période de 24 heures. Mais il n'y a pas de définition unique partagée par les acteurs d'Internet.

Voir SPAM.

4 Voir l'article spécifique à ce sujet.

Buzonfia

SPAM en espagnol.

3.4. C

Canular

Le courrier électronique est utilisé comme moyen pour répandre des canulars de tous ordres qui s'appuient souvent sur les faibles connaissances techniques du grand public. On trouve toutes sortes de plaisanteries plus ou moins sophistiquées et plus ou moins faciles à identifier, dont des alertes pour de faux virus, des demandes d'aide pour une cause ou une personne n'existant pas. Ce phénomène peut s'étendre dans deux directions spécifiques : la tentative d'escroquerie (comme la fausse demande d'assistance d'un diplomate africain en vue de détourner des fonds[5]) ou la légende urbaine (un type de canular qui se propage tout seul en s'appuyant sur les peurs largement partagées dans la société, comme certaines alertes à propos de virus inexistants ou ces courriers qui finissent généralement par une formule du genre « c'est extrêmement important, il faut que vous fassiez passer cette information à tous vos amis »).

D'excellentes références (où l'on peut facilement utiliser le moteur de recherche pour vérifier si le message que l'on a reçu est bien un canular) :

Nom du service	*Remarques*
Le site Hoaxbuster, « le chasseur de canulards » (http://www.hoaxbuster.com/)	En français, et chaudement recommandé à tous - y compris les non techniciens.
CERT (http://www.cert.org/other_sources/viruses.html#II)	En anglais.
CIAC (http://www.ciac.org/)	En anglais.

Et la plupart des vendeurs d'anti-virus (dont le votre) dispose de ce type d'information sur leur site web. Par exemple, chez Symantec US :

http://www.symantec.com/avcenter/hoax.html

Canter & Siegel

En avril 1994, deux avocats de Phoenix (Arizona, USA) ont posté un nombre considérable de messages proposant leurs services (essentiellement inutiles, d'ailleurs) pour participer à la loterie organisée par le gouvernement américain en vue de la distribution d'un lot de *green cards* (cette carte est nécessaire pour tout étranger désirant travailler aux USA). Ils avaient fait cette publicité manuellement sur plusieurs groupes de discussion Usenet, mais le 12 avril, avec l'aide d'un

5 Curieusement, en 2001-2002, on trouve un nombre considérable d'enfants de Laurent Désiré Kabila qui « apparaissent » dans ce genre de courriers électroniques.

programmeur, ils ont bombardé *tous* les groupes de discussion Usenet (soit plusieurs milliers de groupes et des centaines de milliers d'utilisateurs) en quelques minutes.

Il y a plus de détails (en anglais) sur :

http://www.eff.org/pub/Legal/Cases/Canter_Siegel/

Et vous pourrez trouver l'original du SPAM en question sur :

http://www.urbanlegends.com/legal/green_card_spam.html

Le terme de SPAM semble avoir vraiment pris pied dans les jours qui ont suivi cet incident célèbre (tout au moins toutes les victimes l'ont remarqué et retenu) pour décrire ce type de pratique sur Usenet. Il sera repris ensuite pour le courrier électronique.

De plus, on trouvera intéressante la réponse et l'absence d'excuses de l'auteur de ce SPAM (http://www.linuxplanet.com/linuxplanet/tutorials/1096/1/). Essentiellement, l'argument est « pourquoi m'ennuyez-vous ? Je sais bien que tout le monde n'est pas intéressé par ce que je propose mais pourquoi ne pourrais-je pas atteindre [les rares] intéressés par ce moyen si pratique ? ».

Après tout voici encore des gens qui n'ont pas compris le sens de cet aphorisme pourtant si simple : « ma liberté s'arrête là où commence celle d'autrui »...

Carnet d'adresses

La plupart des logiciels de messagerie permettent de stocker en un seul endroit toutes les adresses de courrier électronique de vos correspondants. Comme il s'agit parfois d'adresses peu faciles à retenir cela aide les utilisateurs.

Toutefois, les carnets d'adresses de chaque logiciel sont généralement incompatibles les uns avec les autres. La migration d'un logiciel vers un autre en est souvent compliquée. Mais on peut parfois trouver sur Internet des utilitaires (souvent en freeware) qui font le travail automatiquement.

Cc:

Un des en-têtes les plus « basique » du courrier électronique, le champ Cc: désigne une liste de destinataires secondaires du message qui doivent en recevoir une copie (Cc: signifie littéralement *Carbon Copy* ou *Copie carbone*).

On peut inscrire plusieurs adresses de courrier électronique sur la ligne Cc: en les séparant par une virgule.

Exemple :

Cc: info@SpamAnti.net, John.Doe@stop.abuse.net

Voir aussi Bcc:

CECNS

Correo Electrónico Comercial No Solicitado.

Le nom officiel du SPAM pour les hispanophones.

Censure

Quand on parle de sécurité des communications électroniques (et en particulier de la messagerie), on ne peut s'empêcher d'aborder le thème de la censure qui semble en être considéré comme le pendant.

Le courrier électronique semble n'être ni plus ni moins sensible à la censure que la plupart des autres moyens de communication de personne à personne. On peut remarquer que (de nos jours) les messages circulent très directement d'une machine origine à une machine destinatrice et que les occasions de censure sont assez limitées. Toutefois, dans un contexte professionnel, il est important de noter que les entreprises peuvent (techniquement, et légalement dans la plupart des pays) effectuer un tri dans les messages de leurs salariés. On trouvera par exemple quelques produits listés dans cette encyclopédie qui permettent de réaliser une telle activité (au nom de la sécurité, de la confidentialité et de l'autorité de l'employeur, il est vrai).

Le filtrage (en particulier, quand il est pratiqué par un Fournisseur d'Accès Internet ou un prestataire de service) est parfois accusé d'être une forme de censure. Toutefois, cette accusation provient le plus souvent de spammeurs qui oublient quil s'agit normalement d'un service proposé par le FAI à la demande de l'utilisateur (il s'agit le plus souvent d'une option à valider par l'utilisateur). Cela reste donc assez éloigné de la censure proprement dite qui relèverait plutôt d'une action qui empêcherait autrui de recevoir une information.

CERT

Computer Emergency Response Team, fondé par le DARPA à Fort Lee en réponse à l'incident du vers Morris en 1988, a été créé pour centraliser les efforts de réponse à des incidents informatique de grande ampleur qui comme en 1988. Le groupe est aujourd'hui basé à l'Université Carnegie Mellon à Pittsburgh sous le nom de CERT Coordination Center.

Chain letters

Terme anglais (littéralement « lettres en chaîne ») qui le type de courrier (électronique ou non, d'ailleurs) qui propose d'envoyer un ou plusieurs autre(s) courrier(s) pour faire suite à celui que l'on vient de recevoir. Par exemple, « si vous voulez gagner de l'argent, envoyez cette lettre à 10 personnes et envoyez-moi un Euro ».

Cette pratique (qu'elle implique de l'argent ou pas) est illégale dans la plupart des pays du monde parce qu'elle repose sur la crédulité du public et qu'elle est à l'origine de nombreuses arnaques. L'arrivée du courrier électronique lui a donné un nouvel élan (tout aussi illégal que la version postale).

Les chaînes de ce type présentent de réels dangers qu'on ne peut pas négliger. Elles consomment inutilement des ressources informatiques, elles font perdre du temps à beaucoup de gens, et – pire - elles déforment l'information sur des sujets qui sont souvent importants.

Pour toutes ces raisons, il convient de les détruire, de ne pas les signer, de ne pas les renvoyer ; et si cela est déjà trop tard, de demander à ceux à qui on les a renvoyées de les détruire et de ne pas y donner suite.

chat

Mot anglais commun pour le verbe « discuter ». Il est exceptionnellement traduit par le terme français « tchatche » ou le verbe « tchatcher ».

Système de discussion en temps réel qui présente parfois des similarités avec le courrier électronique mais dont l'immédiateté fait toute la force. Il existe de nombreux systèmes de ce type, mais on pourra noter l'existence de ICQ (aujourd'hui géré par AOL), d'IRC (Internet Relay Chat) ou de MSN Messenger (de Microsoft).

On remarquera que ces systèmes ne sont pas exempts de SPAM. Le phénomène y existe aussi (en particulier sur IRC).

Cheval de Troie

Terme imagé qui décrit un logiciel qui se présente sous une apparence anodine et présente des aspects dissimulés autrement plus dangereux. C'est le terme générique le plus courant que l'on peut employer pour beaucoup de virus qui sont en fait des chevaux de Troie (ils demandent à être exécutés par un utilisateur berné par un aspect inoffensif[6] mais se révèlent contenir une « charge » particulièrement dangereuse).

On remarquera que dans cette définition rien n'indique une quelconque capacité à se propager. L'exemple typique serait celui d'une fausse version de l'utilitaire PKZIP (ancêtre de WinZIP) qui abritait dans les années 1990 un programme particulièrement malicieux. Pour se répandre, il devait être déposé par tel ou tel utilisateur sur des sites de difstribution de shareware, mais il ne faisait aucun effort de ce type par lui-même.

L'origine est évidemment le cheval de bois de l'Illiade d'Homère. Il servit à Achille et à ses compagnons pour s'emparer de la ville de Troie qui résistait pourtant à tous les assaults directs.

Clé publique

Certains moyens de cryptographie utilisent ce qu'on appelle un algorithme « à clé publique ». Cette technique repose sur une asymétrie mathématique qui permet de publier une clé (ou un mot de passe) qui permet de coder un message pour le rendre illisible à quiconque sauf au propriétaire de la clé (et de ses éléments internes réputés inaccessibles).

Ainsi PGP permet de publier une clé publique personnelle qui se présente généralement comme un bloc de caractères. Vos correspondants utilisent votre clé pour encrypter leurs messages et vous êtes ainsi le seul à pouvoir les lire.

Cette approche qui présente de gros avantages pratiques (par rapport aux systèmes et aux algorithmes traditionnels, dits « à clé privée », qui doivent absolument préserver le secret de la clé normalement utilisée par tous) qui en ont fait une méthode de choix aussi bien pour le courrier électronique que pour les transactions bancaires.

Client-serveur

Voir aussi web-based e-mail.

Cloudmark

Cette jeune société de San Francisco propose une technologie de reconnaissance des SPAMs qui repose sur la coopération P2P (pair-à-pair ou *peer-to-peer*). Les participants envoient/échangent les copies des SPAMs qu'ils reçoivent par un protocole proche de celui à l'origine de Napster. Cela peut vouloir dire quelques millions de personnes collaborant à la lutte contre le SPAM.

http://www.cloudmark.com/

CMS

Cryptographic Message Syntax. Le format interne d'un message S/MIME.

6 Un programme pour afficher des image coquines, par exemple.

CNIL ou Commission Nationale de l'Informatique et des Libertés

Cette Commission instituée en France par la Loi n° 78-17 du 6 janvier 1978 (dite loi « Informatique et Libertés ») est une des armes les plus puissantes mises en place dans un pays occidental par l'intermédiaire du corps législaltif pour défendre le citoyen dans son interaction de plus en plus quotidienne avec l'informatique. Autorité administrative indépendante (son statut est proche de celui du Conseil Supérieur de l'Audiovisuel (CSA), de la Commission des Opérations de Bourse (COB), ou encore de la Commission d'Accès aux Documents Administratifs (CADA)), elle a six missions principales :

- recenser les fichiers
- contrôler et vérifier sur place
- réglementer
- garantir le droit d'accès
- instruire les plaintes
- informer le public et les entreprises

A mon avis, la simple existence de la CNIL est une bénédiction pour les internautes français qui disposent d'un soutien officiel de poids dans la lutte pour préserver la vie privée face aux nouvelles technologies de l'information et de la communication. Même si ses moyens restent encore limités, ses pouvoirs sont importants et utilisés de manière responsable.

D'autres pays établissent progressivement une législation nationale similaire et des institutions proches. Quelques unes des plus marquantes dans les pays francophones sont les suivantes :

- Belgique : Commission de la Protection de la Vie Privée (http://www.privacy.fgov.be/)
- Canada : au niveau fédéral - Commissaire à la protection de la vie privée : (http://www.privcom.gc.ca)
- Canada : Québec - Commission d'accés à l'information : (http://www.cai.gouv.qc.ca)
- Suisse : préposé fédéral à la protection des données : (http://www.edsb.ch/)
- Suisse : canton de Zürich : (http://www.ktzh.ch/dsb/)

On trouvera des informations plus précises sur le site web de la CNIL :

http://www.cnil.fr/
Hors de France : http://www.cnil.fr/thematic/indextd3.htm

On remarquera que dans le cadre de son action contre le SPAM, la CNIL a annoncé le 10 juillet 2002 l'ouverture d'une boîte-à-lettres spécialement destinée à recevoir les copies des SPAMs reçus par les internautes français : SPAM@cnil.fr. Cette boîte-à-lettres sera probablement utilisée dans le futur pour lancer des actions en justice contre les spammeurs (et fournir des arguments solides et fondés).

Coalition Against Unsolicited Commercial Email (CAUCE)

Une organisation internationale de personnes qui luttent contre le SPAM. De nombreux comités locaux/nationaux : EuroCAUCE, CAUCE Canada, CAUCE India, CAUBE.AU (Australie). Très sensibles aux problèmes de législation attachés à ce fléau.

Toutefois, on notera que cette organisation connait en 2001-2002 une forte baisse d'activité en Europe (sauf peut-être en Allemagne).

Collecte d'adresses

Une question souvent posée par les victimes du SPAM : « mais comment ont-ils pu obtenir mon adresse pour me bombarder de ces insupportables messages de courrier électronique ? ».

On peut considérer que les moyens sont très nombreux, mais les plus courants sont les suivants :

- ramassage d'adresses présentes sur les sites web publics ou semi-publics,
- ramassage des adresses présentes dans les messages que vous avez envoyés sur une liste de messagerie mal protégée,
- ramassage des adresses présentes dans les messages que vous avez envoyés sur un groupe de discussion,
- reconnaissance de l'adresse de courrier électronique que vous avez indiquée en installant votre navigateur web (Internet Explorer est installé en même temps que le logiciel de messagerie et il fournit l'adresse sur simple demande du site web),
- reconstruction de votre adresse de courrier électronique à partir d'autres éléments publics (comme la première lettre de votre prénom et votre nom)[7],
- collecte directe par des sites web particulièrement peu scrupuleux (vérifier toujours que le site qui vous demande votre adresse vous indique bien l'usage qu'ils comptent en faire).

Cette liste n'est pas exhaustive. En fait, il faut être véritablement paranoïaque pour ne jamais divulguer son adresse de courrier électronique à des tiers - d'autant plus que certaines opérations exigent de fournir votre adresse.

Comments:

Un en-tête non-standard à forme libre. Le cas le plus courant est celui de « Comments: Authenticated sender is <spammer@spamhaus.com> ». Dans tous les cas, le caractère totalement libre du contenu (en général, le logiciel de messagerie permet de saisir manuellement le contenu du champ) ne permet pas de déterminer grand chose.

Voir aussi Authenticated sender.

On rencontre aussi un cas particulier de commentaires courants insérés automatiquement soit par un logiciel de courrier électronique soit par une passerelle :

```
Comments: Sender has elected to use 8-bit data in this message.
  If problems arise, refer to postmaster at sender's site.
```

Il indique l'utilisation d'un format de caractères qui peut poser des problèmes et qui serait utilement remplacé par l'usage d'un format MIME.

7 C'est plus rare, mais dans certains cas, cela est étonnament éfficace.

Compression

Comme les messages transportés par courrier électronique sont de plus en plus gros, les techniques de compression sont couramment employées dans les messages. Il est habituel de compresser un fichier attaché, par exemple.

La compression consiste à utiliser une technique mathématique (souvent très complexe mais dissimulée dans un logiciel spécifique) pour transformer un ensemble de données numérique en un ensemble équivalent mais plus petit en exploitant les redondances dans les données. Par exemple, il sera plus facile de dire « cent fois zéro » que d'écrire les cent caractères 0. Tout l'intérêt de cette technique est de réduire le volume de données à transférer (dans un message par exemple) tout en autorisant le retour à l'original sans perte d'information (ou dans certains cas avec une perte d'information contrôlée et sans gravité).

Parmi les méthodes de compression les plus connues, on citera ZIP (le nom d'un utilitaire de compression sur PC, plus qu'une véritable méthode), LZW (les initiales de ses inventeurs) ou JPEG (une norme de compression d'image qui s'applique bien à des photographies)[8].

Confidentialité

On ne le répètera jamais assez : la majorité des messages qui circulent sur Internet circulent en clair. Ils sont potentiellement lisibles par pratiquement n'importe qui. En pratique, l'accès est un peu plus restreint que cela et on peut considérer que la disponibilité est à peu près la même que pour le téléphone (rarement encrypté) mais avec des phénomènes spécifiques comme le stockage temporaire plus ou moins long de certaines copies des échanges (essentiellement pour des raisons techniques, mais en France aussi parce que les Fournisseurs d'Accés Internet sont tenus de conserver des archives d'un an à la disposition de la Justice).

Conseil de l'Union Européenne

Le 6 décembre 2001, lors de sa réunion sur les Télécomunications, le Conseil de l'Union Européenne a adopté une position très claire contre le SPAM. L'autorisation préalable des internautes devra être obtenue, à quelques exceptions près.

Pour information, le représentant du Luxembourg s'est singularisé en votant contre.

La décision a ensuite été présentée au Parlement Européen pour vote d'une loi en accord avec cette décison (Mai 2002). Le vote par le Parlement Européen la rend applicable. Au moment, de la rédaction de cet article, le vote a été positif et il ne reste plus que la rédaction de la Directive Européenne correspondante pour assurer la mise en place définitive de cette législation.

Cette décision (et la Directive associée) constituent un précédent considérable dans la lutte contre le SPAM, au sens où il s'agit de la première réglementation d'ampleur significative à s'opposer au SPAM. Cela met le SPAM hors-la-loi dans toute l'Union Européenne, soit une proportion notable du réseau Internet.

http://ue.eu.int/fr/summ.htm

8 Les lecteurs les plus attentifs (ou les mieux renseignés) auront remarqué que la compression ZIP n'existe pas à proprement parler mais qu'il s'agit d'un ensemble de techniques de compression de la famille Lempel à laquelle appartient également le LZW cité.

Content-Description:

Un des nombreux en-têtes qui font partie de la définition du codage MIME. Il sert à marquer la partie du message avec une description lisible par l'utilisateur. C'est souvent utilisé à la manière du Subject: d'un message.

Exemple :

Content-Description: Sick Mail Newsletter – 3/4/01

Content-Disposition:

Indique si la portion MIME du message doit être présentée dans le corps du message (in-line) ou comme un attachement. Cet en-tête sert également à suggérer un nom de fichier en cas de sauvegarde de l'attachement.

Voir le RFC 1521.

Content-Id:

Un des nombreux en-têtes qui font partie de la définition du codage MIME. Il est particulièrement utilisé pour construire des documents complexes en HTML. Il donne à une partie de message une référence qui est utilisable par le reste du message (l'usage le plus courant est sans doute de permettre - techniquement parlant - l'inclusion d'images).

Exemple :

Content-ID: <bord180-.JPG>

Content-Location:

Certains messages ne comportent pas l'ensemble du message, mais une ou plusieurs parties qui doivent être retrouvées ailleurs par le logiciel de messagerie du detsinataire. Dans ce cas, ils peuvent utiliser cet en-tête non-standard (et rarement supporté) pour indiquer l'URI où trouver le contenu nécessaire.

Content-Return:

Un en-tête qui permet de choisir d'ajouter le corps du message au rapport de non-livraison d'un message (dans le cas où celui-ci n'est pas bien arrivé à son destinataire). RFC 1327.

Voir aussi X400-Content-Return:.

Content-Transfer-Encoding:

Un des nombreux en-têtes qui font partie de la définition du codage MIME. Il sert à indiquer le type de codage utilisé dans une partie du message.

Exemples :

Content-Transfer-Encoding: 8bit
Content-Transfer-Encoding: quoted-printable

Content-Type:

Un des nombreux en-têtes qui font partie de la définition du codage MIME. Il sert à indiquer le type des caractères qui ont été employés pour l'écriture du message (ou de cette partie du message).

Exemple (le plus courant dans le cas d'un texte utilisant des caractères latins éventuellement avec des lettres accentuées) :

Content-type: text/plain; charset="ISO-8859-1"

Contrat électronique

Depuis 2001 et les décisions de la Commission Européenne, des contrats peuvent être établis de manière électronique de la même manière que par l'intermédiaire des autres moyens de transmission à distance (fax, téléphone, etc.)

Ceux qui sont intéressés par cet aspect légal et législatif sont invités à se reporter aux législations nationales des pays européens concernés. Dans la plupart des cas, il y est décrit le type d'échanges qui doit être assuré pour confirmer et valider un contrat électronique établi dans ces conditions.

Control:

En-tête normalement réservé aux messages Usenet (ne devrait pas apparaître dans les en-têtes de messages de courrier électronique).

Corée (2000-2002)

Ce pays se distingue ces dernières années en étant la plus forte concentration mondiale de connexions à haut débit. Cet honneur s'accompagne d'une conséquence importante pour les analystes du phénomène SPAM. Le haut débit (ADSL ou cable) favorisant traditionnellement des connexions permanentes avec des adresses IP fixes ou presque, les utilisateurs grand public étant le plus souvent très peu sensibilisés aux problèmes de sécurité, ce record est illustré par la présence d'un nombre exceptionnel d'open relays qui sont utilisés (ne faudrait-il pas dire « exploités » ?) par de nombreux spammeurs. C'est là un exemple flagrant de l'écart entre les responsabilités de *tous* les acteurs d'Internet et les connaissances souvent très limitées dont ils disposent pour assumer ces responsabilités.

Par ailleurs, et plus traditionnellement, de nombreux entrepreneurs de petite envergure s'imaginent que leur PC connecté par ADSL est la solution à toutes leurs préoccupations commerciales.

Importantes nouvelles locales (qui indiquent combien le pays se préoccupe du problème du SPAM - même si ce n'est pas de la meilleure manière à mon avis) : la Commission du Commerce Coréenne a lancé un grand programme d'opt-out au niveau du pays pour permettre aux citoyens d'inscrire leur numéro de téléphone et leur adresse e-mail sur une liste devant les « protéger » contre les SPAM. De plus, depuis juillet 2002, les publicitaires qui envoient du SPAM doivent indiquer clairement (en coréen, on peut le supposer) « publicité pour adulte » dans le titre du message de courrier électronique qui contiendrait du sexe ou de la violence; et les déclarations erronnées (qui évitent la détection par un automate de filtrage) comme « advertise.ment » (pub.licité en anglais) sont devenues illégales. L'amende est de 5 millions de Won. Enfin, le gouvernement sud-coréen envisage de mettre en place des mesures permettant de limiter le volume de SPAM qui quitterait le pays (certains autres pays utilisateurs d'Internet se plaignent avec une régularité qui *ennuie* les autorités locales).

Pour ceux qui lisent le coréen dans le texte : http://www.spamcop.or.kr/
http://www.cyberprivacy.or.kr/

Corps (ou corps de texte)

Les E-mails contiennent deux parties essentielles : des en-têtes (ou headers), et un corps de texte. Le corps de texte contient le texte de la correspondance.

Courrier électronique

Un merveilleux moyen de communication entre les personnes. Par l'intermédiaire de quelques ordinateurs et de quelques logiciels, il devient possible d'échanger des messages (essentiellement textuels) dans un temps relativement court (entre le fax et le courrier postal) et avec une simplicité qui s'améliore de jour en jour depuis l'introduction d'Internet comme média d'interconnexion de nombreux ordinateurs.

Pour avoir des informations sur le premier courrier électronique de l'histoire, on se reportera à l'article sur Ray Tomlinson.

Courrier-rebut

Autre nom (francophone et probablement d'origine québecoise) donné au SPAM.

Coût du SPAM

Le SPAM a un coût ; un coût diffus et réparti, mais un coût tout de même.

Pour les utilisateurs : le SPAM demande à détruire un nombre parfois considérable de messages après en avoir lu quelques lignes (ou le sujet). Même pour ceux qui n'en reçoivent pas eux-mêmes, les incidents relativement nombreux liés aux exagérations des spammeurs entraînent des problèmes partagés par tous.

Pour les Fournisseurs d'Accés Internet : le SPAM occupe de la place dans les boîtes-à-lettres. Cet espace se traduit par un volume plus important des disques durs qui servent à l'archivage des boîtes-à-lettres et par une bande passante qui doit être un peu plus importante qu'autrement nécessaire. Cet aspect est - essentiellement - reporté sur les clients sous la forme de coûts plus élevés des abonnements.

Pour les responsables marketing : dans un contexte de plus en plus sensible au sujet du SPAM, certains responsables parfaitement honnêtes et respectueux de la nétiquette sont parfois victimes d'amalgames et de confusions.

Pour les adminsitrateurs de services de courrier électronique : ils sont obligés de maintenir en permanence un niveau élevé de sécurité de leurs systèmes sous peine d'être très rapidement victime d'un viol de relais. Il n'est pas rare que cela se traduise par plusieurs jours d'interruption de service et des coûts de l'ordre de plusieurs dizaines d'hommes-jours (sans compter la perte d'exploitation de l'entreprise).

Pour Internet : le volume de SPAM est tel qu'il est devenu possible de considérer qu'une part mesurable d'Internet est consacrée uniquement au transport de ces pourriels.

Pour la société : ce coût diffus est celui des « mauvais traitements » infligés rapidement à des internautes qui sont encore en phase de découverte d'un média dont la connaissance sera probablement une nécessité dans les années futures. Nombre de débutants sont rapidement rebuttés par ces comportements plus proches du Far West que de la « bonne société ». C'est ainsi que de nombreuses personnes sont davantage exclues (ou exclues plus longtemps) des bénéfices[9] apportés par Internet.

Ainsi, selon une étude commandée par la Commission européenne, les abonnés à l'Internet paieraient, à leur insu, un montant estimé à 10 milliards d'euros par an en frais de connexion, cela uniquement pour recevoir des messages non sollicités.

9 Le montant de ces bénéfices n'est guère important ici, du moment que l'on admet que c'est une perte que de ne pas profiter d'Internet.

Crédit

Toutes les formes de crédit (bancaire ou pas, immobilier ou à la consommation, etc.) sont généreusement représentées dans le SPAM. Là où il y a de l'argent, on trouve des gens pour vouloir en profiter avec un moyen aussi bon marché que le SPAM.

Cybersurveillance

Analysant les réactions et réflexions suscitées par son rapport d'étude de mars 2001 sur la cybersurveillance des salariés dans l'entreprise, la Commission Nationale de l'Informatique et des Libertés (CNIL) a proposé aux employeurs et aux employés des secteurs privé et public des solutions concrètes. Parmi les points les plus novateurs figure la désignation d'un délégué à la protection des données personnelles, qui à terme pourrait devenir le « correspondant informatique et libertés » dans l'entreprise.

Ajoutons que les entreprises qui ont fait ces derniers mois « la une » des journaux dans des affaires de cybersurveillance considèrent presqu'unanimement que les répercutions ont été rarement positives (au minimum, il a fallu faire un gros effort d'information auprès des employés et/ou des candidats à l'embauche).

Voir aussi l'article intitulé « espionnage du courrier électronique ».

Cryptographie

L'étude des pratiques qui permettent de sécuriser les données. Le champ d'application se sépare traditionellement en deux parties *privacy* [ou vie privée] (éviter l'accès sans autorisation) et *authentication* [ou authentification] (prouver l'origine d'un message ou prouver l'identité du lecteur avant d'autoriser la lecture d'un message).

Cyberout Email Services

Une société amie de Cyber Promotions Inc. qui a semble-t-il utilisé les serveurs ou les services de Sanford Wallace. Elle est toujours considérée par certains comme une « filiale » de Cyber Promotions Inc. - sans doute à tort.

Cyber Promotions Inc. (ou Cyberpromo)

La société crée par Sanford Wallace (auto-proclamé roi du SPAM dans les années 1990) pour gérer ses activités de spammeur et de revendeur de services de SPAM.

La Cyber Promo FAQ :

http://www.sdmedia.net/argarg/spam901.html

On remarquera que les domaines utilisés par Cyber Promotions Inc. ou ses clients (qui apparaissent dans cette FAQ) sont définitivement tâchés par cette appartenance. Quelles que soient vos intentions, si vous envisagez d'acheter un de ces noms de domaine, préparez-vous à ne pas pouvoir en faire un usage normal devant les défenses organisées pendant la lutte contre Sanford Wallace et qui sont certainement restées en place en de nombreux endroits (vous risquez de ne jamais pouvoir communiquer avec certains correspondants à cause de cela).

3.5. D

DARPA (ou parfois ARPA)

Defense Advanced Research Projects Agency. Un département du gouvernement américain qui s'occupe de haute technologie pour la défense de ce pays. Ils ont financé un nombre considérable de projets dont Arpanet qui est ensuite devenu Internet, le protocole TCP-IP, les projets Berkeley d'Unix BSD v4.x, et « Secure DNS ».

Date:

Les messages de courrier électronique sont estampillés d'une date d'expédition. Elle apparaît dans l'en-tête Date: qui est présent sur tous les courriers.

Toutefois, on remarquera utilement que cette date est fixée par le logiciel de rédaction du courrier. Elle est également dépendante de la notion de date telle que comprise par l'ordinateur du rédacteur. Il y a donc plusieurs raisons courantes pour que la date indiquée soit plus ou moins fausse. Les plus courantes sont : l'horloge de l'ordinateur de l'expéditeur n'est pas à l'heure (éventuellement fausse de plusieurs jours ou plusieurs mois) ; le décalage horaire entre les machines de l'expéditeur et du destinataire n'est pas correctement pris en compte par l'un ou l'autre de leurs logiciels ; un spammeur peut souhaiter modifier cette date pour faire apparaître son « message » devant les autres courriers reçus par ses victimes.

Décoder et décodage

Processus qui permet de faire passer un ensemble de données (par exemple, un fichier attaché ou une pièce jointe) de l'état illisible utilisé pour le transporter à un état lisible par l'utilisateur final.

Delivered-To:

Cet en-tête est normalement rempli par le dernier MTA (Mail Transport Agent) au moment où le courrier électronique est déposé dans une boîte-à-lettres physique.

Exemple :

```
Delivered-To: roumazeilles@noos.fr
```

Certains MTA sont connus pour ne pas effectuer correctement ce marquage, mais il est globalement respecté.

Delivery-Date:

En-tête non standard (RFC 1327) qui marque l'heure et la date de livraison du message à son destinataire.

Démon (ou daemon ou demon)

Type de programme qui fonctionne tout seul en arrière-plan du reste du fonctionnement d'un ordinateur. De nombreux logiciels serveurs de messagerie fonctionnent ainsi.

Le terme provient d'Unix mais a été repris dans de nombreux autres contextes. Les termes de service ou d'agent système se rencontrent également (souvent sur des systèmes Microsoft).

Denial of Service (DoS)

Le terme français équivalent (déni de service) est beaucoup moins employé que l'original anglais. Pourtant, il aurait l'avantage d'être très clair pour décrire un type d'attaque électronique dont l'objectif est de retirer à la victime la possibilité de se servir d'un ou plusieurs moyens informatiques qui sont la cible de l'attaque DoS.

Tous les types de service peuvent être victimes de ce type d'attaque qui consiste à saturer la cible avec des demandes plus ou moins réelle au point de la rendre incapable de traiter son activité normale. Dans le cas d'un serveur de courrier électronique ou d'un utilisateur de courrier électronique, une attaque DoS peut par exemple consister à bombarder la victime avec un nombre considérable de messages (on peut penser à des chiffres allant de quelques milliers à quelques millions de messages). L'agresseur s'attend à ce que la victime soit submergée par le déluge de messages, devenant ainsi incapable de traiter son courrier d'une manière normale. Dans les cas extrêmes, on peut s'attendre à ce qu'un serveur soit amené à s'arrêter totalement, ou à ce qu'un utilisateur ne trouve d'autre porte de sortie que de détruire ou faire détruire tous les messages reçus (utiles ou non).

De nombreux autres types d'attaques DoS sont envisageables (et utilisés).

Le terme DDoS (Distributed Denial of Service ou déni de service distribué) est utilisé dans le cas où l'attaque est coordonnée entre plusieurs ordinateurs rendant ainsi presqu'impossible de s'en prémunir. Les attaques de ce type qui ont été observées sur des serveurs de grande taille se sont révélées très efficaces et sont considérées comme un véritable moyen de guerre électronique contre lequel il est difficile de se défendre.

DES (ou Data Encryption Standard)

Algorithme cryptographique qui est au coeur de nombreux standard nationaux et internationaux. Il est aujourd'hui considéré comme insuffisant pour les applications véritablement sérieuses (à la suite d'avances techniques et théoriques). Le « double DES » est aussi insuffisant, le « triple DES » est considéré comme très fiable, tout comme le récent AES (Advanced Encryption Standard)[10].

Toutefois, ces positions extrêmes ne doivent pas masquer le fait que pour la discrétion de communications qui ne risquent pas une attaque directe et résolue (la grande majorité des communications individuelles), tous ces algorithmes présentent des avantages notables. Les indications que je donnent doivent sans doute plutôt être utilisées comme des informations sur la direction qui sera prise - à mon avis - par la technologie dans le futur proche.

DGCCRF

Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes. L'organisme public – en France – qui s'occupe de la défense des consommateurs. Cet organisme s'occupe de plus en plus de la consommation dans le cadre d'Internet et des fraudes ou tentatives de fraudes qui l'utilisent.

http://www.finances.gouv.fr/DGCCRF/

Digital signature

Voir signature numérique.

10 On remarquera qu'actuellement l'AES est plutôt une famille d'algorithme puisqu'il reste encore cinq candidats (Mars d'IBM, RC6 de RSA, Rijndael de deux chercheurs belges, Serpent issu d'une large collaboration internationale [britanniques, norvégiens, israëliens], Twofish de Counterpane).

Disclose-Recipient:

Détermine si les adresses des autres destinataires peuvent être révélées à un destinataire normal du message. RFC 1327. En général (hors du contexte X.400), cette clause est parfaitement gérée par l'emploi de To:, Cc: et Bcc:).

Distribution:

Un en-tête non standard prévu pour limiter la distribution d'un message sur une base géographique ou organisationnelle.

DL-Expansion-History-Indication:

Trace des différentes listes de messagerie traversées par le message (quand il y en a plusieurs). RFC 1327.

DMA

Direct Marketing Association.

L'association qui regroupe la plupart des entreprises américaines qui pratiquent le marketing direct (pas nécessairement par Internet). Très conscients des possibles réactions négatives du public face au SPAM, la DMA essaye d'organiser le marketing direct sur Internet dans l'intérêt de ses membres. Nombreux sont les activistes anti-SPAM à considérer la DMA comme un véritable adversaire parce qu'ils favorisent des pratiques qui semblent trop favorables aux spammeurs.

DNS

Domain Name Services.

Le service qui assure la correspondance sur Internet entre un nom de domaine (comme *USA.net* ou *SpamAntiFr.cjb.net*) et l'adresse IP appropriée.

Le nom de domaine « en clair » est un confort considérable pour les internautes, mais les machines elles-même n'utilisent pas vraiment ces noms. Elles préferrent les adresses IP. Le DNS assure cette correspondance de manière transparente dans la plupart des cas.

Certains services RBL utilisent une extension des protocoles DNS pour diffuser en temps réel l'information sur les sites qui sont dans les listes noires.

Un livre conseillé :

DNS and BIND, 4th Edition

By Paul Albitz, Cricket Liu

4th Edition April 2001

Editions O'Reilly

0-596-00158-4, 622 pages

Domino

Ce serveur est le pivot de la famille Lotus Notes.

Drop box

Ce terme anglais (traduction approximative « boîte à laisser tomber ») décrit un type de boîte-à-lettres souvent utilisé par les spammeurs. Il s'agit d'ouvrir une boîte-à-lettres chez un fournisseur (gratuit de préférence). Cette boîte est prévue (dès l'origine) pour ne pas être véritablement utilisée. Par exemple, il peut s'agir du compte e-mail qui va servir à envoyer le SPAM. Ou bien d'une adresse à contacter pour « se voir retiré de la liste de messagerie ».

En réalité, le spammeur sait que ce compte sera fermé d'office par le fournisseur d'accès dès qu'il sera connu qu'il a servi à produire du SPAM. Mais le spammeur n'en a cure. Soit il l'a déjà employé et n'en a plus besoin (utilisé pour envoyer le SPAM), soit il n'a pas vraiment l'intention de jamais l'utiliser (pratiquement aucun spammeur ne souhaite s'encombrer avec le traitement des messages de mécontentement des internautes qui ne souhaitent plus recevoir ces messages. Voir le compte fermé par le fournisseur d'accès donne une excellente excuse pour ne faire aucun effort...).

DUL

Dialup List (liste de connexions dial-up ou modem)

Certains filtres contre le SPAM utilisent une telle liste. Il s'agit de reconnaître les mails venant de gens qui se connectent par un modem (donc chez un FAI traditionnel) mais envoient directement leur mail sans passer par le serveur SMTP de leur FAI. Cela repose sur le fait que les spammeurs qui envoient eux-mêmes leur SPAM (sans utiliser un viol de relais) ne peuvent guère passer par le serveur SMTP de leur FAI. La quasi-totalité des FAIs refusent de voir transiter des millions de courriers électroniques en provenance d'un seul utilisateur. Le spammeur doit donc trouver une autre solution et si la connexion n'est pas chère il peut installer directement un serveur sur son propre PC. Cela produit des courriers électroniques dont les en-têtes sont reconnaissables : ils passent par un serveur SMTP ou un MTA dont l'adresse fait partie des blocs d'adresses IP qui sont allouées dynamiquement par un FAI. Si l'on connaît ces blocs d'adresses (c'est le rôle des DULs), on peut assez facilement les intercepter.

On peut trouver des renseignements complémentaires sur http://mail-abuse.org/dul/.

Dynamique

Est considéré comme dynamique une information qui évolue dans le temps. Dans le cas particulier d'une adresse IP, on peut disposer soit d'une adresse IP statique, soit d'une adresse IP dynamique. Une adresse IP dynamique est le plus souvent une adresse qui est affectée pour un temps donnée ou pour la durée d'une opération simple. Par exemple, un utilisateur qui se connecte à son Fournisseur d'Accès Internet par modem se verra probablement affecter une adresse IP dynamique pour la durée de sa connexion. Cette adresse sera différente à sa prochaine connexion.

Dans le cas général, cela n'a guère d'importance puisque l'utilisateur a une adresse techniquement claire pour la durée de sa connexion à Internet. Toutefois, une adresse IP dynamique complique singulièrement la tâche de mettre en place un serveur. Cette caractéristique rend les spammeurs qui utilisent une adresse IP dynamique particulièrement difficiles à retrouver y compris quand on a pu remonter jusqu'à leur adresse IP, puisqu'il en change régulièrement.

3.6. E

Echelon

Un système à très grande échelle d'espionnage des communications électroniques organisé par les Etats-Unis avec l'assistance de plusieurs autres pays (dont la Grande Bretagne, le Canada, l'Australie et la Nouvelle- Zélande). Le système est considéré capable d'intercepter une très grande part des communications téléphoniques et électroniques du monde (y compris en en particulier les communications par courrier électronique), en faisant appel à des moyens très divers qui vont de la pose d'écoutes sophistiquées à l'utilisation de satellites[11].

11 Et en s'appuyant sur le fait qu'une très grande partie des communications électroniques mondiales passe à un moment ou à un autre par des équipements qui sont physiquement aux Etats-Unis. Les autres membres du réseau permettent une couverture mondiale encore plus efficace.

Malgré des dénégations américaines, les autorités européennes qui ont déjà publié plusieurs rapports publics sur le sujet suspectent une utilisation dans le domaine de l'espionnage industriel (et pas seulement dans celui de la lutte contre la criminalité).

EFF

Electronic Frontier Foundation.

Une association de San Francisco qui regroupe des membres soucieux de préserver leurs droits de pensée, de parole, ou à partager des idées en utilisant des moyens électroniques. L'EFF se concentre sur l'identification des menaces contre les droits fondamentaux liés au droit d'expression à l'époque des nouvelles technologies.

http://www.eff.org/

EHLO

Voir « HELO ».

elm

Un logiciel client de gestion de courrier électronique développé par HP mais qui a ensuite été mis dans le domaine public. Un des premiers logiciels de ce type à fonctionner en mode écran, en présentant les messages les uns au dessus des autres, etc. Un véritable ancêtre qui continue à évoluer puisque la version la plus récente a intégré MIME.

EMA

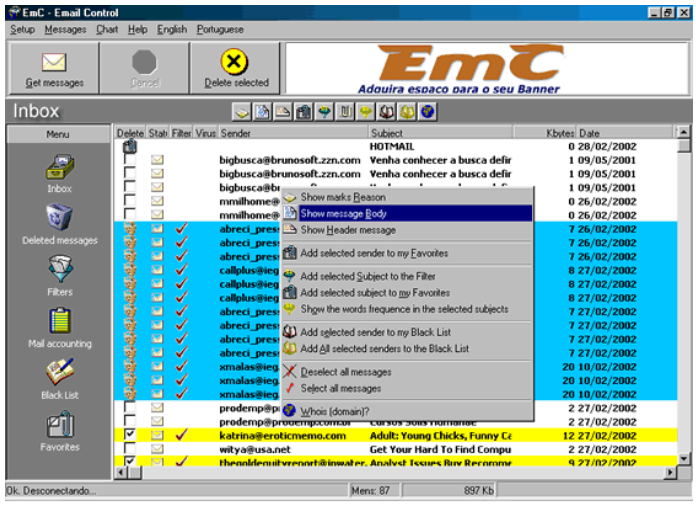
Electronic Messaging Association.

Une organisation de vendeurs et d'utilisateurs de nombreux types de messagerie électronique.

e-mail

Abréviation la plus courante de « Electronic Mail » (ou « courrier électronique » en anglais). Ce terme a aussi conquis le monde francophone grâce à sa simplicité. Toutefois, dans l'encyclopédie, j'ai choisi de privilégier l'expression plus totalement francophone de « courrier électronique ».

Email Control



Un logiciel de traitement et de filtrage du courrier électronique qui fonctionne sous Windows et qui coopère avec votre client de messagerie (apparemment quel qu'il soit).

Je ne l'ai pas testé personnellement, mais les caractéristiques semblent alléchantes et on me l'a chaudement conseillé. Seuls bémols pour ce freeware, la gratuité se paye par de la publicité dans le logiciel lui-même, et le site est dans un anglais de cuisine qui est une traduction automatique du portugais.

http://www.abreuretto.com/anti-spam/

en-têtes

Les E-mails contiennent deux parties essentielles : des en-têtes (ou headers), et un corps de texte. Les en-têtes contiennent les informations nécessaires à l'identification du courrier (par exemple, auteur et destinataire) et à son acheminement (par exemple, priorité de distribution).

Certains logiciels de courrier électronique peuvent présenter les en-têtes sous une forme compacte qui ne fait pas apparaître la plupart des informations peu utiles à un lecteur humain.

Exemple d'en-têtes d'un e-mail :

```
Return-Path: <roumazeilles@usa.net>
Delivered-To: roumazeilles@noos.fr
Received: (qmail 6438897 invoked by uid 0); 9 Dec 2001 04:47:51 -0000
Received: from unknown (HELO urdvg135.cms.usa.net) ([204.68.25.135]) (envelope-sender
<roumazeilles@usa.net>)
        by 212.198.2.71 (qmail-ldap-1.03) with SMTP
        for <roumazeilles@noos.fr>; 9 Dec 2001 04:47:51 -0000
Received: (qmail 22375 invoked from network); 9 Dec 2001 04:55:42 -0000
Received: from uadvg009.cms.usa.net (165.212.10.9)
  by outbound.postoffice.net with SMTP; 9 Dec 2001 04:55:42 -0000
Received: (qmail 2566 invoked by uid 0); 9 Dec 2001 04:47:00 -0000
Message-ID: <20011209044700.2565.qmail@uadvg009.cms.usa.net>
Received: from cpdvg001.cms.usa.net [165.212.8.10] by uadvg009.cms.usa.net via mtad (34FM.0700.19.01A)
                with ESMTP id 656FLieU10962M09; Sun, 09 Dec 2001 04:46:52 GMT
Received: from Spam [24.126.225.134] by cpdvg001.cms.usa.net via mtad (34FM.0700.19.01A);
```

```
                Sun, 09 Dec 2001 04:47:51 GMT
From: "peterov" <peterovg2v2k2@vhost.usa.net>
Subject: Test message
To: roumazeilles@usa.net
Content-Type: text/plain
Date: Sat, 8 Dec 2001 20:43:33 -0800
X-Priority: 3
X-Library: Indy 8.0.25
```

Les mêmes en-têtes présentés sous une forme simplifiée (et considérablement plus lisible parce que ne contenant que les seuls en-têtes habituellement utiles) :

```
From:       "rouliakov" <rouliakovg2v2k2@vhost.usa.net>
Subject:    Test message
To:         roumazeilles@usa.net
Date sent:  Sat, 8 Dec 2001 20:43:33 -0800
```

On notera que les en-têtes réduits ne sont pas d'une grande utilité pour identifier la véritable origine d'un courrier électronique, surtout dans le cas d'un SPAM qui cherche à dissimuler sa source. Il est donc impératif de savoir retrouver (ou faire apparaître) les en-têtes complets d'un courrier.

Enclosure

Ce terme anglais est parfois utilisé à la place de « attachement ». La distinction est suffisamment ténue et peu comprise pour garantir l'absence de traduction convenable de la différence.

En fait, « enclosure » fait référence à un type de pièce attachée où le document est envoyé dans un message de courrier électronique séparé alors que le terme attachement fait plutôt référence à une pièce jointe qui est comprise dans le corps du message lui-même.

Encoder et encodage

Processus qui permet de faire passer un ensemble de données (par exemple, un fichier attaché ou une pièce jointe) de l'état lisible par l'utilisateur final à son état illisible utilisé pour le transporter.

EPIC

Electronic Privacy Information Center.

Centre créé à Washington D.C en 1994 pour attirer l'attention du public sur le sujet des libertés civiques, pour protéger la vie privée, le 1er Amendement de la Constitution Américaine, les valeurs de la même Constitution.

http://www.epic.org/

Errors-To:

Indique une adresse de courrier électronique où renvoyer les erreurs rencontrées et dont la cause est considérée comme chez l'expéditeur. Un exemple typique est l'erreur « no such user » (utilisateur inexistant). Comme l'expéditeur préferre souvent recevoir les erreurs à la même adresse que celle qu'il a utilisée pour écrire (comportement par défaut), cet en-tête (légitime pourtant) n'est pas très courant.

ESMTP

Extended SMTP.

Une extension de SMTP qui définit un cadre dans lequel des tiers peuvent faire des ajouts au standard SMTP.

Espionnage du courrier électronique

En France, une entreprise peut légalement espionner le courrier de ses employés (essentiellement à la condition de le dire clairement). On pourra se reporter utilement au rapport de la CNIL (http://www.cnil.fr/thematic/docs/entrep/cybersurveillance2.pdf) qui traite de la cybersurveillance sur les lieux du travail.

Toutefois, les emails privés restent de nature privée. Cela n'empêche pas une entreprise d'y accéder dans certaines conditions.

La source de futures batailles juridiques dans les entreprises françaises pendant que cettejurisprudence se mettra en place.

En Belgique, la situation semble plus simple puisque l'employeur n'est pas autorisé à placer sous écoute ou enregistrer les conversations téléphoniques, ni à lire ou copier les lettres ou les courriers électroniques de ses employés.

Toutefois, il convient d'insister sur le fait que je ne suis pas juriste et que ces aspects évoluent rapidement dans un univers où la technologie se transforme au moins aussi vite que la jurisprudence se constitue.

Espionnage industriel

En 1999, les entreprises Fortune 1000 ont signalé un total de 45 milliards de dollars de pertes dues à des actes d'espionnage industriel (source : « Trends in Proprietary Information Loss », American Society for Industrial Security et PricewaterhouseCoopers, 1999).

La première source de fuites était et reste le personnel de l'entreprise (action de l'intérieur). Internet en général et le courrier électronique en particulier facilite certaines formes de collecte d'information par les entreprises concurrentes. On citera les forums de discussion (ou les listes de messagerie électronique) ou les courriers électronique envoyés un peu trop rapidement ou à des destinataires mal choisis (diffusant ainsi des informations internes ou confidentielles, comme un rapport interne ou une liste de clients). Dans certains cas, on remarquera que le concurrent qui organise l'activité d'espionnage pourra utiliser des formes d'ingéniérie sociale (voir cet article) pour mener certains employés à divulguer involontairement des informations confidentielles.

ETRN

Une extension de type ESMTP qui permet de gérer une queue de messages à distance (tel que des serveurs de messagerie qui ne sont pas connectés à Internet).

Eudora mail

Logiciel de courrier électronique shareware produit par Qualcomm Enterprises.

Eudora est souvent considéré comme un outil assez facile à utiliser. Il a connu son heure de gloire à l'époque où il était principalement diffusé gratuitement. L'existence d'Outlook Express gratuitement dans les configuations Windows standard lui a retiré beaucoup d'intérêt (et de clients) sur cette architecture.

Il existe des extensions gratuites qui permettent de lui faire parler français, allemand et quelques autres langues. Ce logiciel existe aussi bien pour Mac que pour PC.

http://www.eudora.com/

example.com, example.net et example.org

Ces noms de domaines ne peuvent pas être enregistrés (ils sont réservés par avance et de manière définitive). Leur seul usage est dans les documentations où cela évite d'employer des noms et des adresses qui peuvent réellement appartenir à quelqu'un.

Excessive Cross Posting (ou ECP)

La pratique de l'envoi d'un même message sur un trop grand nombre de groupes de discussion Usenet.

Voir aussi la « FAQ: Current Usenet Spam thresholds and guidelines » (http://www.killfile.org/faqs/spam.html) qui décrit les seuils habituellement considérés pour définir cette pratique.

Excessive Multi Posting (ou EMP)

A strictement parler, la pratique de l'envoi répété d'un même message sur un groupe de discussion Usenet. Le terme SPAM est le terme moins technique plus couramment employé.

Exchange

Serveur de messagerie de Microsoft.

Probablement, le plus couramment utilisé après sendmail (d'après le SMTP Gateway Survey présenté à http://www.bbv.com/SMTP-Survey.htm).

http://www.microsoft.com/

Excuses de spammeurs

Sanford Wallace (voir Spamford) a beaucoup utilisé l'argument de la protection des forêts et de l'économie de papier dans son usage du SPAM.

Même si l'on peut admettre l'argument (en faveur du courrier électronique et pas seulement du SPAM), il reste clair que cela était une tactique pour colorer positivement ses actions négatives, au milieu de l'activité qui se concentrait sur lui.

Mais un nombre considérable de noms de domaines déposés par Sanford Wallace et sa société Cyber Promotions Inc. portaient la marque de cet argument : savetrees.com, savepaper.com.

De la même manière, Sanford Wallace s'est beaucoup appuyé sur le 1er Amendement à la Constitution Américaine (qui précise et défend la liberté d'expression). Ce second argument semble plus fort parce qu'il a été employé devant des juridictions qui ne sont pas toujours insensibles à sa portée.

Cyber Promotions Inc. a ainsi déposé les domaines 1stamend.com, fight4rights.com, nocensorship.com, etc.

Plus sérieusement, la plupart des spammeurs (comme l'on fait les avocats Canter & Siegel dès les premières réactions à leur SPAM historique) s'appuient sur un argumentaire simple du type : « si vous m'interdisez de spammer, vous me coupez de mes clients potentiels ». La notion de responsabilité (liée à l'impact et au coût social démesuré quand on multiplie ces incidents) n'est pas prise en compte : « je sais bien que certains destinataires ne sont pas intéressés, mais les autres ont un besoin *critique* de mon

SPAM ». Le rapport entre les nombres de destinataires (intéressés ou pas) n'entre pas en ligne de compte.

Exim

Exim est un MTA pour Unix développé par l'Université de Cambridge (Royaume Uni) et distribué gratuitement selon la license dite « GNU General Public License ». Il est similaire à Smail3 mais a été particulièrement étendu pour faciliter le filtrage du trafic malvenu ou frauduleux.

http://www.exim.org/

Un livre conseillé :

Exim - The Mail Transfer Agent

De Philip Hazel

Juillet 2001

Editions O'Reilly

0-596-00098-7, 632 pages

exmh

Un logiciel client de gestion de courrier électronique développé par Brent Welch, anciennement chez Xerox PARC puis Sun. Une application un peu étonnante écrite en Tcl/Tk avec un excellent support du MIME.

Expression régulière

Une forme de définition qui est souvent employée pour décrire une *forme* à rechercher dans un texte. Cette forme a été créée pour pouvoir aller plus loin que demander « rechercher les caractères TOTO », mais autoriser des demandes plus complexes comme « rechercher un caractère alphabétique quelconque ». Cette dernière demande pourra être exprimée par [a-zA-Z].

La forme (parfois peu lisible, il est vrai) est utilisée pour sa puissance. Elle a été popularisée sur MS-DOS par l'emploi des caractères particuliers que sont ? et * quand on désigne des noms de fichiers (? signifie *n'importe quel caractère* et * signifie *n'importe quel nombre de n'importe quel caractère*). Toutefois, les puristes (dont je suis !) considèrent cette forme très réduite, présentée par Microsoft dès les premières versions de l'antique MS-DOS, comme une dégénerescence de la richesse et de l'élégance naturelle des expressions régulières.

On retrouve souvent les expressions régulières employées par des filtres de courrier[12] ou dans la configuration d'un programme comme sendmail.

On utilise parfois (et de manière interchangeable) les abréviations de regex ou regexp (abréviations naturelles de l'anglais « regular expression ») pour désigner les expressions régulières.

NOTE 1 : les programmeurs qui recherchent des expressions régulières particulièrement en relation avec l'usage du courrier électronique sont invités à se reporter au paragraphe 9.1 « Expression régulières utiles » (page 159).

NOTE 2 : les programmeurs qui recherchent une bibliothèque capable de gérer les expressions régulières peuvent s'intéresser à YGrep Search Engine que j'ai développée moi-même dans une autre vie (plus de détails sur http://www.roumazeilles.net/ygrep.htm). Je ne vois pas pourquoi je me priverais de me faire une petite publicité ici ;-)

Extra-terrestres (message reçu des extra-terrestres)

La SETI League, Inc. (société qui s'efforce de trouver des traces d'intelligence extra-terrestre dans les émissions radio qui peuvent être perçues sur Terre) affirme que la NASA a reçu à l'adresse abuse@NASA.gov le message de courrier électronique suivant intitulé « QUIT SENDING US YOUR

12 En particulier, quand ils sont écrits dans une langage comme PERL qui inclut les expressions régulières, ou quand un programme les reconnaît bien comme Pegasus mail.

STUPID JUNK (*arrêtez de nous envoyer vos cochonneries ridicules*) » . Traduit approximativement en français, cela donne :

Humains --

Veuillez arrêter de nous envoyer vos transmissions non sollicitées et vos déchets. Nous avons reçu plusieurs objets métaliques transportant des artefacts, des dessins simplistes, et des disques qui produisent des bruits lorsqu'on les gratte avec une aiguille à extrémité de diamant. Nous ne savons pas qui est « Bach », mais dîtes-lui qu'il devrait penser à changer de profession. Honnêtement, nous recevons des milliers de trnasmissions non-sollicitées et d'objets provenant de sociétés comme la votre en train de devenir une vraie plaie ; alors, arrêtez cette pratique immédiatement ou nous serons obligés de nous plaindre auprès de votre prestataire de service et d'information, ou plus simplement, de détruire votre stupide planète et toutes ses formes de vie stupides. Envoyez vos déchets aux Gezor - ils ont la classe et l'intelligence de clazins bouillis. Mes respects,

Elinzoa Glppaducc
Coordinateur du Traitement de l'Information
Le Shati-Makal

La NASA aurait immédiatement annulé les plans d'expédition d'une capsule temporelle contenant un CD du succés de Ricky Martin, « Livin' La Vida Loca », et une copie VHS de la série « Friends ».

http://www.setileague.org/articles/alienmsg.htm

3.7. F

FAI

Voir Fournisseur d'Accès Internet.

Fax

Curieusement, cette technologie dont le courrier électronique se vante d'avoir marqué l'arrêt de mort est aussi une référence importante en matière de SPAM. De nombreux pays ont mis en place une législation spécifique qui interdit l'usage du fax pour envoyer de la publicité non solicitée. A ma connaissance, la France ne dispose pas d'une telle législation spécifique mais la loi Informatique et Libertés serait applicable selon certains juristes.

Le principe reposait déjà sur l'idée qu'une part très importante du coût de diffusion de la publicité était ainsi supporté par le destinataire (qui doit payer le papier et l'encre - ce qui à l'époque des fax thermiques à papier spécial ou de ceux utilisant des rouleaux encreurs spécifiques était une dépense très importante).

Cette référence légale constitue souvent la base de la proposition de lois en vue de réguler l'envoi de SPAM. Après tout, le SPAM tombe dans la même situation : une grande part de la dépense est du côté du destinataire[13].

13 Ce qui n'est pas du tout le cas de la publicité par courrier postal où le coût le plus important est porté par l'expéditeur sous la forme des frais de port, des coûts de papier et d'enveloppe, des frais d'impression en quantité, etc. Cette distinction est importante puisqu'elle force le diffuseur à cibler son envoi pour « rentabiliser » sa dépense, alors que les spammeurs ont seulement intérêt à élargir la cible (puisque le coût marginal d'un envoi supplémentaire reste quasiment nul).

Fax:

Un en-tête non standard indiquant le numéro de fax de l'expéditeur.

Fichier attaché

Un fichier peut être attaché à un courrier électronique (c'est-à-dire joint à celui-ci pour être adressé à un correspondant). Le fichier est alors encodé (généralement au format MIME) pour être transporté dans de bonnes conditions et pour pouvoir être relu facilement par le destinataire.

Filtrage

Action qui consiste à ne pas seulement diriger le courrier électronique en fonction de sa destination, mais en fonction de son contenu. Par exemple, un serveur de messagerie peut filtrer contre les virus en appliquant un logiciel de détection de virus aux messages et en détruisant les courriers qui sont reconnus comme « infectés ».

De même, un logiciel de courrier électronique peut - à la demande de son utilisateur - automatiquement trier les messages dans différents dossiers (par exemple, en fonction de leur origine).

Cette pratique est mise en oeuvre - avec plus ou moins de bonheur - pour se débarrasser du SPAM. Pour cela, on utilise souvent des listes noires.

Quelques méthodes

La plus efficace :

Les filtres faits sur mesure par vous en fonction des SPAMs que vous recevez. C'est un peu plus compliqué, mais ça finit par être très efficace (au moins au niveau de votre compétence dans la création de ces filtres - qui va aller en s'améliorant avec l'expérience).

Très utile :

Des filtres automatiques sont peut-être proposés par votre fournisseur de courrier électronique. Le plus souvent, c'est une option qu'il faut valider volontairement (par exemple, c'est le cas chez USA.net). Ces filtres se veulent aussi efficaces que possible sans jamais perdre un message utile. Par conséquent, en cas de doute, ils préferrent laisser passer le message. Cela donne une efficacité élevée mais laisse passer une part significative de SPAM. Si c'est applicable chez votre Fournisseur de courrier électronique, je vous recommande vivement d'en profiter.

Presqu'inutile :

Essayer de se « désabonner » en suivant les liens de type « remove ». Ils ne fonctionnent généralement pas (pour toutes sortes de raisons techniques ou non) et quand ils fonctionnent ils sont souvent utilisés pour enregistrer le fait que votre adresse de courrier électronique existe bien (le problème des listes d'adresses qui sont revendues ici ou là reste qu'elles contiennent beaucoup de vieilles ou fausses adresses. Si on peut réduire ce taux, on augmente la valeur de la liste. En répondant, vous aidez donc les spammeurs à vous spammer).

Inutile :

Filtrer les spammeurs individuellement sur l'adresse d'expédition. Cela fait longtemps que les spammeurs n'utilisent plus qu'exceptionnellement leur propre adresse en clair. Soit ils créent une boite à lettres pour le seul envoi, soit ils falsifient le message pour faire croire qu'il provient d'une adresse (vraie ou fausse) qui n'est pas la leur.

Firewall

Voir Pare-feu.

Flamme (ou flame)

Message particulièrement déplaisant et/ou insultant. On parle de flame war (guerre de flammes) quand de tels messages sont rapidement échangés entre plusieurs utilisateurs (généralement sur une liste de messagerie).

Recourir à ce mode de communication est considéré comme très négatif par la plupart des utilisateurs. Et pourtant, cela arrive couramment.

For-Comment:

Un en-tête non-standard qui est sensé désigner les destinataires qui doivent avoir une action à la réception du message.

Voir aussi For-Handling:.

For-Handling:

Un en-tête non-standard qui est sensé désigner les destinataires qui doivent avoir une action à la réception du message.

Voir aussi For-Comment:.

Fournisseur d'Accès Internet (FAI)

Pour accéder à Internet et en utiliser tout ou partie, il faut disposer d'un fournisseur d'accès. Dans le cas le plus courant, il s'agit de la société qui fournit un numéro de téléphone auquel connecter votre modem.

Il est courant que le FAI soit aussi fournisseur d'autres services. Le plus souvent, un Fournisseur d'Accès Internet offrira également un service de courrier électronique (une ou plusieurs boîtes-à-lettres et au moins un serveur d'envoi de courrier).

Forward ou transférer

Dans le contexte d'un logiciel de courrier électronique, action qui consiste à transférer à quelqu'un d'autre un message préalablement reçu.

Exemple :

Jean,
Je te signale que Pierre organise une réunion pour
laquelle tu n'as pas pu recevoir l'invitation
Henri
> Il y aura une réunion du service lundi matin.
> Je n'ai pas l'adresse de Jean.
> Peux-tu lui forwarder l'invitation pour moi ?
> Pierre

Comme on peut le constater ici, on observe parfois l'utilisation du verbe de franglais « forwarder ».

Forwarding

Certains prestataires de courrier électronique fournissent un service très spécifique de « forwarding ». Il s'agit de fournir une adresse de courrier électronique (par exemple, SPAM.Anti@USA.net[14]) et de s'assurer que tout le courrier qui est reçu sera immédiatement renvoyé vers une autre adresse de courrier électronique.

C'est très pratique pour plusieurs raisons, mais je voudrais citer les suivantes. Même si vous changez de Fournisseur d'Accès Internet, votre adresse ne change jamais (il suffit de changer l'adresse de destination). Par exemple, il y a quelques années, quand je suis passé de Compuserve à Magic Online, je n'ai eu à prévenir aucun de mes correspondants qui ont continué à utiliser l'adresse SPAM.Anti@USA.net sans même savoir que j'avais « déménagé ». J'avais simplement fait une petite opération de reconfiguration de mon compte chez USA.net.

De plus, cet intermédiaire dans ma communication avec le reste du monde permet de garder une certaine discrétion sur l'emplacement eaxct de ma boîte-à-lettres (non qu'il soit impossible de la retrouver, mais une petite distance supplémentaire n'est pas désagréable dans le cas de SPAM.Anti).

Pendant quelques années, on a pu rencontrer ce genre de service à titre entièrement gratuit. Mais bien que son fonctionnement soit très peu consommateur de ressources, il est totalement gratuit puisque le prestataire n'a même pas l'occasion de présenter de la publicité à ses clients (vous n'allez sur le site du prestataire qu'exceptionnellement – quand vous changez de boîte-à-lettres, par exemple). Il est donc devenu rare de trouver gratuitement ce genre de service.

14 Mon **ancienne** adresse de courrier électronique pour la lutte contre le SPAM (Veuillez ne plus l'utiliser ; elle ne fonctionne plus aujourd'hui. La nouvelle/actuelle est yr@SpamAnti.net et n'utilise pas du tout le même mécanisme).

Je vous signalerai uniquement les suivants :

Nom du service	*Remarques*
USA.net (http://www.usa.net/)	Service payant. Très stable, très sérieux. Je l'utilise personnellement depuis 1996.
POBoxes (http://www.poboxes.com/)	Service payant. Un des prestataires les plus anciens sur ce marché.
Ulimit (http://www.ulimit.com/)	Service gratuit qui fournit simultanément une redirection d'URL (de site web) et un *forwarding* des adresses de courrier électornique. Semble sérieux.
CJB net (http://www.cjb.net/)	Service gratuit de redirection web qui comporte une option de *forwarding* des adresses de courrier électronique. Très stable et très sérieux.
No-IP (http://www.no-ip.com/)	Service gratuit de redirection web qui comporte une option de *forwarding* des adresses de courrier électronique.

Le site anglophone http://www.internetemaillist.com/Forwarding/ présente utilement un certain nombre de ces services.

Free Software Foundation

La *Fondation du Logiciel Libre* est le promotteur et le producteur (au sens cinématographique du terme) du projet GNU. C'est aussi l'organisation la plus active du monde du « logiciel libre ».

http://www.gnu.org/

Freeware

Logiciel distribué gratuitement. Attention, la distribution gratuite n'implique pas que vous pouvez faire tout ce que vous voulez avec le logiciel. Il est donc conseillé de lire attentivement la notice de license qui accompagne certainement le logiciel concerné.

Fréquence des messages (sur une liste de messagerie)

Je conseille vivement aux gestionnaires d'une liste de messagerie de prévenir les abonnés dès leur inscription (ou dès la demande de confirmation) du volume de courrier électronique normalement produit par la liste de messagerie (un message par mois, un par jour, 10 par jour, 100 par jour, cela change tout). Evitez de surprendre vos « clients ».

Si la fréquence est basse ou très basse, je conseille de toujours envoyer un message par mois. Cela permet d'éviter que les destinataires oublient complètement qu'ils sont inscrits à la liste (ce genre d'oubli génère des plaintes qui sont - de fait - injustifiées, mais n'en produisent pas moins un niveau d'instatisfaction qui n'est pas souhaitable). Cela permet aussi de fournir les informations qui permettent de modifier l'abonnement (changement d'adresse, désinscription, suspension, etc.). Il est toujours possible de trouver une information (même mineure) à fournir mensuellement aux abonnés (ou alors la liste n'a probablement pas lieu d'être).

From (en-tête sans suffixe :)

C'est le « envelope From » (From de l'enveloppe).

From:

Parmi les en-têtes habituels d'un courrier électronique, on rencontre l'en-tête From: qui désigne l'expéditeur du courrier. Il est suivi d'une adresse e-mail selon le RFC 822.

Exemple :

From: info@SpamAnti.net

C'est le « message From: » (From: du message).

Federal Trade Commission (FTC)

La commission fédérale américaine qui s'occupe des problèmes liés au commerce. Elle a une activité spécifique et exemplaire en matière de SPAM. En particulier, on notera que la FTC assure une collecte permanente de SPAM (envoyés par les citoyens internautes à l'adresse uce@ftc.gov).

Dès 1998, cela avait permis de réaliser des statistiques et de décrire une classification des « douze salopards » du SPAM :

- les affaires (ou escroqueries) commerciales,
- gagner de l'argent en envoyant du SPAM,
- les lettres-chaînes,
- travailler chez soi,
- santé et régimes,
- argent facile,
- recevez quelque chose de gratuit,
- investissement et Bourse,
- décodeurs de télévision,
- prêts et crédits,
- reprises de crédit,

- gain de vacances gratuites.

Si cette liste devait être reconstruite aujourd'hui, il est très vraisemblable qu'elle ne changerait pas vraiment malgré les années passées, à l'exception de la catégorie qui était étonnament encore absente à cette époque (et qui a beaucoup enflé depuis) : le sexe et la pornographie.

3.8. G

Garantie

Contrairement à ce que beaucoup croient, le courrier électronique tel que défini par les RFC 821 et suivants n'apporte aucune garantie de distribution ou de lecture. Il n'est pas techniquement anormal qu'un message de courrier électronique soit perdu sans aucun message d'erreur.

Toutefois, il est exact que, malgré les réelles limitations techniques, une garantie de distribution est aujourd'hui attendue par la plupart des utilisateurs et les fournisseurs d'accès s'efforcent de véritablement respecter cet engagement non-écrit.

Gateway

Voir passerelle.

Generate-Delivery-Report:

Un en-tête qui permet de forcer l'envoi d'un rapport de livraison d'un message (dans le cas où celui-ci est bien arrivé à son destinataire). RFC 1327.

GIF

Format d'image qui autorise une légère compression, cette technologie présente plusieurs contraintes dont la limitation à 256 couleurs seulement et l'existence d'un brevet détenu et défendu par Unisys. Malgré cela, il s'agit certainement du format d'image le plus répandu sur Internet à ce jour.

Pour compresser des images photographiques on lui préferre souvent le format JPEG. Le format PNG est une tentative de remplacer GIF par un format complètement libre et disponible dans le domaine public.

Voir aussi JPEG.

GILC

Global Internet Liberty Campaign. Une organisation internationale qui défend la liberté d'accès et d'usage des technologies de cryptographie.

Global Internet Liberty Campaign

Voir GILC.

Projet GNU

GNU is not Unix.

Le projet de Richard M. Stallman et la Free Software Foundation de créer un clone du système d'exploitation Unix qui soit totalement libre et gratuit. Le produit le plus connu est GNU/Linux qui est le fruit des travaux combinés du projet GNU et du noyau Linux de Linus Torvalds.

http://www.gnu.org/

GNU/Linux

Le système d'exploitation que beaucoup de gens appellent Linux devrait en fait être nommé GNU/Linux comme le répète inlassablement Richard Stallman. Il s'agit en effet de l'amalgame (réussi) du noyau Linux et du système d'exploitation GNU construit par la Free Software Foundation sous le nom de « projet GNU ».

Il s'agit d'un système d'exploitation d'ordinateur gratuit, de grande qualité, et qui pourrait prendre des parts de marchés à MS-Windows de Microsoft. Il est distribué (plutôt que vendu) par des sociétés comme Red Hat, Mandrake ou Debian pour un prix dérisoire (généralement de quelques Euros seulement).

Golden Mallet

Une récompense informelle attribuée par la communauté anti-SPAM à un de ses membres les plus méritants. En général, la désignation se fait par acclamation ou consensus. Le premier Golen Mallet est allé à AfterBurner (le pseudonyme de l'administrateur du bureau des abus chez le FAI américain Erols).

GPL

GNU General Public License (ou License publique générale GNU).

Une forme de license de logiciel qui repose sur le principe (défendu par GNU et Richard Stallman) que le logiciel doit être libre. Les particularités les plus frappantes d'une telle license sont à mon avis, tout d'abord, que le logiciel peut être copié à volonté, il est fourni avec son source, et ensuite, que le logiciel peut être modifié à volonté, mais les modifications doivent toujours être livrées dans des conditions au moins aussi avantageuses que la GPL (donc au moins avec les sources et la liberté de copie et de modification).

Le principe permet de favoriser l'extension du phénomène du « logiciel libre » par « contamination ». Et il est au coeur du développement mondial du phénomène.

Il existe également une version légèrement différente (la GLPL ou GNU Lesser General Public License) qui s'applique à certaines bibliothèques de logiciel. Et on rencontre aussi une FDL (GNU Free Document License) pour un traitement similaire des manuels et des documentations.

http://www.gnu.org/licenses/licenses.html

Traductions non officielles :

http://www.gnu.org/licenses/translations.html

Traduction française non officielle :

http://www.april.org/gnu/gpl_french.html

On pourra remarquer le terme de « Copyleft » qui est généralement utilisé pour désigner ce type de license (par opposition au « Copyright » traditionnel).

Gratuit

Internet est un espace où l'on trouve de nombreux services gratuits. Le courrier électronique n'y fait pas exceptione et il est facile d'obtenir une adresse de courrier électronique sans bourse délier. Il existe essentiellement deux types d'opportunités. Premièrement, des services de courrier électronique accessibles par le web (voir web-based e-mail). Ils se financent le plus souvent par la publicité affichée sur le site. Deuxièment, des sociétés associent une adresse e-mail à leurs autres services. Cela peut être le cas d'associations pour leurs adhérents, de banques ou de sociétés de crédit pour leurs clients, etc.

Green card ou Green card lottery

Voir Canter & Siegel.

Groupes de discussion

Ce terme français est généralement utilisé pour désigner les forums de discussion Usenet.

On notera l'excellent moteur de recherche Google (héritier du défunt DéjàNews) qui permet d'explorer les groupes de discussion aussi facilement que les sites web.

3.9. H

Hacker

Ce terme a longtemps été utilisé par les passionnés de l'informatique pour désigner ceux d'entre eux qui avaient poussé la passion à un niveau de raffinement culturel qui les distingue du commun des mortels. Toutefois, le terme a été repris et déformé par la presse lorsque certains hackers se sont fait connaître par des actions répréhensibles (cyber-attaques).

Aujourd'hui les deux sens sont souvent mêlés et il est parfois difficile de distinguer l'emploi pour un technophile ultra-compétent et pour un malfaiteur informatique plus ou moins compétent techniquement.

Une remarque importante pour ceux qui envisageraient de flirter avec la limite entre ces deux acceptions du terme. Les entreprises (et les juges) sont parfois très peu compréhensives avec les actes qui touchent à leur sécurité informatique. Un cas typique et qui avait reçu une importante publicité est celui de Randal L. Schwartz. Expert reconnu internationalement du langage PERL (auteur de deux des ouvrages de référence sur le sujet chez O'Reilly), journaliste technique chez Unix Review et Web Techniques Magazine, Schwartz était aussi administrateur système (consultant) chez Intel quand cette société l'a accusé d'actes répréhensibles qui semblaient pourtant relever de son rôle dans la recherche des limites des sécurité des systèmes dont il avait la charge. Il a été condamné à une peine de prison de 90 jours (avec sursis), 480 heures de travail, et 68 000$ de dommages et intérêts pour Intel. Ses frais d'avocat se sont également élevés à plus de 170 000$. La limite est parfois difficile à reconnaître et il est utile d'y réfléchir à deux fois.

Harcélement

La facilité avec laquelle un message peu être envoyé par courrier électronique peut faire oublier les règles élémentaires liées à la préservation des droits d'autrui. En particulier, le harcélement reste répréhensible quand il est pratiqué par courrier électronique. Un internaute français en a fait les frais en 2002 lorsqu'il a tenté de poursuivre une « amie » de ses ardeurs électroniques et s'est vu attaquer par le fournisseur d'accés Internet (Noos) qui a vu ses serveurs envahis par les messages de l'amoureux éconduit.

Hash

La prononciation anglaise la plus courante pour le caractère dièse (#).

Haut-débit

Dénomination qui recouvre (à un moment donné) les technologies qui fournissent un débit plus élevé que la technologie dominante. Par exemple, au moment de la rédaction de cet article (fin 2002), le haut débit en France est représenté par les technologies ADSL et cable qui se partagent environ 20% des internautes. On peut supposer que lorsque l'ADSL aura envahi le marché français, le terme haut-débit sera employé pour des technologies encore plus rapides et en cours d'introduction sur le marché.

Le terme « haut-débit » est la traduction de l'anglais « broadband ».

Headers

Voir en-têtes.

HELO

Le protocole SMTP commence par un échange très reconnaissable entre les deux ordinateurs en cause. Le client « appele » le serveur par quelque chose qui ressemble à :

```
HELO client.fr
```

Le serveur y répond (si tout se passe bien) par :

```
EHLO serveur.fr
```

Le mot EHLO est bel et bien HELO (en anglais, bonjour se dit « hello ») avec deux lettres permutées, une petite facilité de programmation qui est devenu une « marque de fabrique » du protocole SMTP dont toutes les commandes font exactement quatre lettres de long.

Hoax

Le mot anglais pour « canular ». Voir ce terme.

Hors sujet

On dit qu'un message électronique est « hors sujet » quand il est posté sur une liste de messagerie ou un groupe de discussion dont le thème ne correspond pas au contenu du message (par exemple, un message sur les langages de programmation est généralement hors sujet dans une liste de messagerie sur le tourisme dans les villes francophones du Canada).

La plupart des SPAMs ne sont pas hors sujet dans les forums, les listes de messagerie où ils sont publiés[15]. Par contre, ils sont malvenus. A l'opposé, les messages hors sujet sont généralement considérés comme étant une marque de très mauvaise éducation ou comme un manquement important à la nétiquette.

Hotmail

Sans doute le plus gros fournisseur mondial de messagerie électronique accessible par le web (voir web-based e-mail).

HTML

Hyper Text Markup Language.

Il s'agit du langage de programmation dans lequel sont écrits les site web d'Internet. Mais il s'agit aussi d'un langage qui permet de facilement mettre en forme des documents (et donc éventuellement des courriers électroniques). Outlook et Outlook Express ont sans doute été les premiers logiciels de courrier électronique – largement répandus – à employer HTML dans les messages. Les experts du sujet admettent aisément que cela a apporté un ensemble de bienfaits et de problèmes (parfois contradictoires) parmi lesquels on peut citer :

- des messages plus agréables à lire (gestion des polices de caractères) ;
- des messages exagérément lourds (abus d'incorporation d'images) ;
- des messages parfois rendus illisibles (abus des couleurs et de constructions complexes) ;
- des messages souvent peu compatibles avec d'autres logiciels de messagerie ;
- des messages susceptibles de propager de nombreux vers et virus (du fait de très nombreuses failles de sécurité dans l'implémentation de HTML par Microsoft).

Voir Outlook Express.

Host ou hôte

Désigne un serveur ou une machine ayant un usage fixe. La désignation est assez flexible. Curieusement, le terme anglais reste plus employé que la traduction française.

hosts

Une technique relativement efficace pour éliminer de vos communications les spammeurs que vous avez reconnus consiste à faire en sorte de ne plus pouvoir communiquer avec eux. J'apprécie particulièrement cette approche parce qu'elle frappe directement le spammeur « là où ça fait mal ». Personnellement, je refuse d'avoir quelque relation commerciale que ce soit avec un spammeur.

Pour cela, un moyen simple consiste à mettre à jour un fichier qui est présent sur pratiquement toutes les ordinateurs (que ce soit des PC sous Windows, des Mac sous Os-X, des Linux ou des stations de travail) : le fichier hosts. Il liste les correspondances entre des noms de machine ou de domaine et des adresses IP fixes. Si vous le remplissez avec des informations « fausses » pour certains domaines, ceux-ci deviennent essentiellement inaccessibles par votre ordinateur.

Emplacements habituels du fichier hosts selon le type de Système d'Exploitation :

15 Toutefois, de nombreuses listes de messagerie refusent explicitement les messagesà caractère commercial ou les SPAMs.

Système d'Exploitation	*Emplacement du fichier hosts*
Windows 95/98/Me	c:\windows\hosts
Windows NT/2000/XP Pro	c:\winnt\system32\drivers\etc\hosts
Windows NT/2000/XP Pro	c:\winnt\system32\drivers\etc\hosts
Windows XP Home	c:\windows\system32\drivers\etc\hosts
Linux Red Hat	/etc/hosts

Note : sur la plupart des systèmes, sauf Windows 95/98/Me, il vous faudra avoir les droits de l'adminstrateur pour pouvoir modifier ce fichier).

Vous y trouverez généralement une ou plusieurs lignes qu'il est important de conserver au début du fichier sans les changer, comme :

```
127.0.0.1 localhost
192.168.0.2 autre_machine
```

Vous allez rajouter d'autres lignes de la forme :

```
127.0.0.1       www.sale_spammer.com
```

Et ainsi toutes les tentatives d'accéder à ce site www.sale_spammer.com échoueront (ou tomberont sur le site web de votre PC, si vous en avez configuré un) parce qu'elles sont « redirigées » vers l'adresse IP particulière qu'est 127.0.0.1 (cette adresse est un raccourci qui correspond toujours à votre PC).

Certains logiciels d'élimination des publicités utilisent ce truc. Vous pouvez utiliser des listes noires comme celle de SpamAnti.net pour constituer votre propre fichier hosts.

Rappel : surtout n'enlevez pas les informations que vous pourriez trouver déjà présentes dans votre fichier hosts. Ne faites que rajouter des lignes nouvelles à la fin. Les erreurs de ce type se traduisent généralement par de gros problèmes avec votre connexion Internet...

3.10. I

IAB

Internet Architecture Board.

http://www.iab.org/iab

IANA

Internet Assigned Numbers Authority.

L'organisme à but non lucratif qui a longtemps géré les attributions de noms et de numéros pour Internet sous contrat du gouvernement des États-Unis. Cet organisme est maintenant totalement intégré dans l'ICANN.

http://www.iana.org/

ICANN

Internet Corporation for Assigned Names and Numbers.

L'organisme à objet non-lucratif qui gère les attributions de noms et de numéros pour Internet. Cet organisme central dans le fonctionnement d'Internet gère par exemple l'assignation des noms de domaine (voir DNS).

On remarquera que, durant l'année 2001, de nombreuses voix se sont élevées pour contester les conditions de participations à cette organisme. Son caractère démocratique a notamment été contesté vivement[16] dans un contexte où l'ICANN s'efforçait de ménager internautes individuels et grandes corporations publiques ou privées.

http://www.icann.org/

ICMP

Internet Control Message Protocol. Le protocole utilisé pour envoyer de très petits messages de service sur Internet. En particulier, il est employé par ping.

IDP

Internet Death Penalty (en français « peine de mort Internet »).

Voir UDP.

IEEE

Institute of Electrical and Electronic Engineers. Une association professionnelle qui, entre autres, rédige des standard. Sa présence est notable sur Internet.

http:://www.ieee.org/

IESG

Internet Engineering Steering Group.

Le groupe qui surveille le fonctionnement de l'IETF et qui détermine les propositions qui deviendront des standard.

http://www.iesg.org/

IETF

Internet Engineering Task Force.

L'organisme membre de l'ICANN qui reçoit les RFC, en débat et les adopte éventuellement. Il s'agit de l'instance la plus technique de l'ICANN.

http://www.ietf.org/

Image

De plus en plus de logiciels de messagerie sont aujourd'hui capables d'insérer des images dans le corps d'un courrier électronique. Cela passe le plus souvent par l'intermédiaire de l'emploi simultané du langage HTML et du codage MIME.

16 Jean-Noël Tronc, conseiller technique du Premier Ministre français Lionel Jospin avait parlé de « démocratie censitaire » en 1999 à Helsinki, en rapprochant les débats sur les règles de participation aux élections du XIXe siècle français et sur les conditions d'élection au conseil d'administration de l'ICANN.

Imail

Une passerelle SMTP de IPSwitch. Probablement, une des plus couramment utilisées après sendmail (d'après le SMTP Gateway Survey présenté à http://www.bbv.com/SMTP-Survey.htm).

http://www.ipswitch.com/

IMAP

Interactive Mail Access Protocol.

Moins courant que POP3, IMAP offre des services très proches (lecture et collecte de messages stockés sur un servuer de messagerie) et présente quelques avantages supplémentaires dont l'accès simultané à plusieurs boîtes-à-lettres et la recherche de courrier en fonction de critères de tris. Il est sensiblement plus complexe à mettre en œuvre que POP3, ce qui explique sa relative rareté. Mais cela est sans doute appelé à changer dans le futur.

Un livre conseillé :

Managing IMAP

De Dianna Mullet, Kevin Mullet

Septembre 2000

Editions O'Reilly

0-596-00012-X, 405 pages

Permet d'accéder à du courrier électronique ou à des messages (éventuellement partagés) sur un serveur de courrier. Les messages peuvent être manipulés sur le serveur sans être déplacés sur l'ordinateur client. Cela favorise l'accès aux messages depuis *plusieurs* ordinateurs.

IMAP est défini par le RFC 2060.

Importance:

Cet en-tête permet de donner un niveau de priorité à un message. Il est assez mal géré (et on lui préferrera les en-têtes Priority: et X-Priority:), mais le principe veut que les correspondances suivantes soient utilisées :

Importance:	*Signification*
Importance: important	Priorité maximale (urgent)
Importance: normal	Priorité normale

Exemple :

```
Importance: normal
```

Voir également Priority:, X-Priority: et X-MSMail-Priority:.

InboxDoctor

Un filtre de SPAM qui fonctionne sur la base de signatures de SPAM qui sont collectées par un réseau de volontaires et fournies aux clients pour reconnaître les messages qui sont des SPAMs.

Comporte également un filtre contre les virus et une mise à jour en ligne.

http://www.inboxdoctor.com/

Inbox Protector

Un outil de filtrage des mails qui fonctionne spécialement avec Outlook et Outlook Express. Il dirige les messages suspects vers un répertoire séparé pour une analyse ultérieure.

http://www.inboxprotector.com/

Ingéniérie sociale

En anglais, social engineering.

Une pratique devenue courante chez les arnaqueurs en tous genres. Elle représente un des risques les plus importants en matière de sécurité informatique parce qu'elle repose non pas sur la destruction d'une sécurité, mais sur l'emploi d'un être humain qui dispose des droits nécessaires. Typiquement, il s'agit de convaincre un utilisateur de faire une action qui semble anodine ou nécessaire et qui va se révéler particulièrement dangereuse.

Par exemple, il s'agit de convaincre un utilisateur d'ouvrir et d'exécuter un fichier attaché à un courrier électronique. C'est sur ce principe que s'est diffusé le virus « I love you » : le titre du message laissait supposer un contenu « intéressant » même si l'origine en était parfaitement inconnue.

La grande difficulté pour se protéger contre cet aspect d'une attaque informatique reste que la faille est rarement compensable par de la technologie et que la formation y joue un rôle important (et coûteux).

Il me paraît clair que, dans les années à venir, les organisations qui se préoccupent peu ou prou de sécurité devront traiter ce risque en priorité. Certaines commencent à le faire en interdisant par exemple la réception de tout courrier électronique contenant un logiciel exécutable (même avec une excellente formation, un utilisateur pourrait encore faire une « fausse manoeuvre » et ouvrir la porte à une agression « de l'intérieur » ou un cheval de Troie).

In-Reply-To:

Cet en-tête optionnel indique la référence (Message-ID:) du message auquel il est répondu. Il est censé permettre une gestion plus facile des courriers par les logiciels qui savent rassembler les messages électroniques et leurs réponses.

Exemple :

In-Reply-To: <3C605A56.17705.353D1BB@localhost>

Voir aussi Message-ID: puisque l'en-tête In-Reply-To: contient des informations qui sont recopiées de l'en-tête Message-ID: d'un message antérieur.

Internet Draft

Traduction approximative : Brouillon Internet.

Un document technique définissant un aspect d'Internet et proposé à la revue par l'IETF (en vue de son adoption comme standard).

Internet Mail Consortium

La seule organisation internationale créée pour gérer le courrier électronique en coopération, en assurer la promotion sur Internet (y compris dans le domaine du commerce électronique).

http://www.imc.org/

Internet Manager

Une ligne de produits de Elron Software qui contient des produits de filtrage d'Internet dont IM Message Inspector qui permet de surveiller les contenus des courriers électroniques (par exemple pour détecter les virus et le SPAM, mais aussi et surtout pour détecter les « fuites » d'information et les « failles » de confidentialité dans une entreprise).

http://www.elronsw.com/

IP

Internet Protocol.

Une méthode pour assurer le transfert d'information entre des réseaux éventuellement incompatibles. Ce protocole est à la base de tout le développement (et du succès) d'Internet comme « réseau de réseaux ».

Voir egalement adresse IP et passerelle.

IPv6 ou IPng

IP version 6 ou IP nouvelle génération.

Le protocole IP a été défini à une époque où Internet était infiniment plus petit et moins complexe qu'aujourd'hui. Il présente donc des limitations qui peuvent rendre difficile son emploi dans le futur.

Une évolution du protocole IP actuel (connu comme IP version 4 ou IPv4) est actuellement en préparation. Son nom le plus courant est IPv6. Elle devrait apporter un nombre important d'améliorations plus ou moins visibles pour un utilisateur normal, dont l'extension considérable du nombre des adresses accessibles tout en restant une extension naturelle de l'exsitant. Actuellement, les adresses IP ne permettent de définir qu'un maximum théorique de 4 milliards d'adresses. IPv6 est prévu pour augmenter ce nombre au point de permettre de disposer d'environ 1500 adresses IP par mètre carré à la surface de la Terre (océans compris). Le spectre de la pénurie d'adresses IP devrait donc en être effectivement repoussé pour un moment.

IPsec ou IPSEC

Internet Protocol Security. Des fonctionnalités de sécurité incorporées directement dans le protocole IP. En cours de diffusion (il est optionnel dans Ipv4, mais il devient obligatoire de l'incoporer dans les implémentations d'IPv6).

IP spoofing

Une technique qui commence à être utilisée par les spammeurs pour dissimuler leur adresse IP à un serveur de courrier électronique (et ainsi circonvenir les mesures de protection éventuellement mises en place).

IPX

Le protocole de Novell Netware quand il est empaquetté ou « tunellisé » dans IP.

IronPort

IronPort est un produit qui ne se contente pas d'identifier les SPAMs (et de les filtrer comme pratiquement tous les logiciels anti-SPAM) ; il identifie aussi les expéditeurs légitimes de courrier électronique (et construit des « listes blanches » d'utilisateurs non-spammeurs). Il repose sur un système

de paiement (une « caution » ou « bond ») et autoriserait à « valider » l'adresse de quelqu'un connu comme « non-spammeur » (et si cela se révèle faux, l'argent est perdu et donné à un tiers).

Iron Port n'y gagnera peut-être pas beaucoup d'argent, mais cette pratique pourrait se révéler un régulateur intéressant en créant un poste de coût dans le système de SPAM (comme pour l'envoi de courrier publicitaire papier).

http://www.ironport.com/

ISDN

Integrated Services Digital Network.

Voir RNIS.

ISOC

Internet Society.

Le plus ancien groupe constitué pour la promotion de l'Internet. Les représentations locales ou nationales portent le joli nom de « chapîtres ».

Il est parfois remarqué que les entreprises ou les administrations sont beaucoup mieux représentées que les internautes individuels dans cet organisme. Mais les chapîtres constituent une capacité de représentation locale qui est largement considérée comme appréciable et inhabituelle.

ISP

Internet Service Provider.

Voir Fournisseur d'Accès Internet.

ISPam

Un Fournisseur d'Accès Internet créé par Sanford Wallace (auto-proclamé roi du SPAM dans les années 1990) pour faciliter la revente de ses services de SPAM.

3.11. J

Java

Langage de programmation qui a été initialement développé pour ses qualités de portabilité (avec lui, il est théoriquement possible d'écrire un programme qui fonctionne identiquement sur diverses plateformes ou ordinateurs habituellement incompatibles). Il a eu un succès certain sur les sites web écrit en HTML et étendus avec des fonctionnalités Java.

Développé par Sun Microsystems, il est aujourd'hui présent (sous des formes pas toujours 100% compatibles) dans des produits de Microsoft comme Outlook Express ou Internet Explorer.

Cf Outlook Express.

Javascript

Langage de programmation qui a été initialement développé pour ses qualités de portabilité (avec lui, il est théoriquement possible d'écrire un programme qui fonctionne identiquement sur diverses plateformes ou ordinateurs habituellement incompatibles). Il a eu un succès certain sur les sites web écrit en HTML et étendus avec des fonctionnalités Javascript.

Plus limité que Java, il est aussi plus facile à employer, plus courant et plus largement représenté. Il est aujourd'hui présent dans des produits de Microsoft comme Outlook Express ou Internet Explorer, ou dans ceux de Netscape comme Netscape Messenger ou Netscape Navigator.

Cf Outlook Express et Nestcape Messenger.

Jello

Après le succés du terme SPAM, certains ont voulu désigner par ce terme culinaire la publication d'un même message sur un trop grand nombre de groupes de discussion Usenet (Excessive Cross Posting ou ECP) combiné à leur envoi répété (SPAM). Le terme est le plus souvent compris, mais n'est plus guère employé.

Voir aussi Velveeta.

Jeux par courrier électronique

Voir « play by mail ».

JPEG ou JPG

Format de compression d'image particulièrement bien adapté aux images photographiques, cette technologie porte le nom du comité qui l'a standardisée : le Joint Photographic Experts Group. Ce format réduit le volume de données à transporter mais au prix d'une perte d'information (normalement non visible à l'oeil) qui n'autorise pas de revenir à l'image d'origine.

Voir aussi GIF.

Junk mail

Terme anglais qui regroupe toutes les formes de courrier électronique désagréable et sans utilité (traduction approximative en français « courrier électronique de poubelle » ou « pourriel »).

JUNKBUSTERS

Une organisation et un fournisseur d'outils qui se préoccupe de préserver la vie privée des internautes en butte au SPAM ou aux publicités sur les sites web, mais aussi à l'envahissement des boites-à-lettre physiques et des fax par la publicité papier. Les logiciels de Junkbusters sont relativement efficaces et précis, même si un peu difficiles à utiliser pour le commun des mortels.

http://www.junkbusters.org/

JunkTrap

Un logiciel de filtrage du courrier électronique basé sur procmail et réalisé par Heddy Boubaker. Il permet de filtrer les SPAMs (ou tout au moins un bon nombre d'entre eux).

http://www.tls.cena.fr/~boubaker/JunkTrap/

3.12. K

Kabila

Le défunt président de la République Démocratique du Congo, Laurent Désiré Kabila (et son hypothétique famille tentaculaire) est régulièrement utilisé par des arnaqueurs qui exploitent le courrier électronique pour renouveller la bonne vieille arnaque nigériane. Rien de très original[17], mais étonnament efficace.

Le principe : un quelconque dignitaire ou fonctionnaire véreux a réussi à détourner des fonds. Il a besoin de votre aide pour y accéder. Dans un premier temps il vous sera demandé un numéro de compte en banque pour déposer temporairement les fonds (contre un fort pourcentage, souvent plusieurs dizaines de millieurs de dollars à gagner au passage). Mais rapidement (et avant de voir la couleur de l'argent), les choses se compliquent et il faut faire l'avance d'une somme faible en comparaison avec le gain[18]. Les gogos - qui sont déjà engagés dans une opération frauduleuse comme ne manquera pas de le faire remarquer l'escroc éventuellement devenu maître-chanteur - se retrouvent saignés dans l'espoir fou d'une somme mirobolante (qui peut s'accroître au cours du développement de l'arnaque).

Le SPAM ne sert là qu'à toucher encore plus de pigeons (pardon, « de victimes potentielles ») sans changer la structure de base de l'escroquerie. L'arnaque nigériane avait connu un tel succés dans les années 1970-80 que certaines banques dont le nom était trop souvent associé à ces messages téléphoniques ou postaux ont dû publier des placards d'explication dans les grands journaux européens de finance (comme Investir en France ou le Financial Times en Angleterre). Il n'en reste pas moins étonnant que des gens apparemment normaux acceptent de se lancer dans un montage acrobatique et quasiment comique pour participer à ce qui est immédiatement présenté comme une escroquerie des plus évidentes. Ah ! l'appat du gain poussera vraiment certains à toutes les extrémités en matière de malhonnêteté !

Ceux qui voudraient avoir des exemples et des détails sur le mode de fonctionnement peuvent consulter les deux sites suivants (en anglais) :

http://thespamletters.com/letter.php?spamID=101&sortBy=da&start=0&search=Nigerian

http://www.savannahsays.com/kizombe.htm

Keywords:

Un en-tête rare mais standardisé (par le RFC 822, pas moins) qui permet d'ajouter des mots-clef pour aider la recherche ultérieure dans une base de données de courrier électronique.

Killfile

La plupart des lecteurs de forums de discussion Usenet disposent d'une fonction qui est particulièrement utile pour filtrer les messages provenant d'un auteur particulièrement désagréable. De manière générale, on l'appelle le « killfile » (ou « fichier de tueur » ou « fichier d'élimination »). On trouve parfois aussi le nom de liste de Bozos ou filtre à Bozos.

17 Les services fiscaux, douanniers, et bancaires connaissent parfaitement ce type d'arnaques qui ne change que très peu de semaine en semaine depuis 20 ans.

18 Dans les cas extrêmes, les escrocs peuvent aller jusqu'à pousser la victime à se rendre dans un pays lointain où il sera possible de procéder à un enlèvement en bonne et due forme avec demande de rançon comme cela arrive parfois. Le simple chantage (remarquez que le simple fait de commencer à participer relève de la criminalité : détournement, recel, etc. ; cela donne une bon point d'appui pour faire chanter la victime) ne leur suffit pas toujours !

KMail

Le logiciel de messagerie qui est généralement présent avec l'interface graphique KDE dans les distributions Linux les plus courantes. Comme beaucoup de produits Linux, il est gratuit, très complet, très puissant et un peu complexe pour les utilisateurs novices.

3.13. L

LART

Loser Attitude Readjustment Tool. Outil mythique à utiliser pour corriger l'attitude ou le comportement d'un perdant (généralement pour redresser un utilisateur désagréable, dangereux, ou stupide). L'abréviation complètement opaque pour le commun des mortels permet à des technophiles de se moquer quasiment publiquement de certains utilisateurs. Une des preuves de l'existence d'une culture propre à l'environnement informatique des hackers (au sens noble du terme).

Voir aussi loser et luser.

LDA

Local Delivery Agent.

Logiciel (ou ordinateur) qui assure la livraison de courrier électronique. Le meilleur exemple est certainement procmail.

LDAP

Lighweight Directory Access Protocol.

LDAP est un moyen standard pour accéder à un répertoire (une base de données qui est prévue pour être lue plus souvent que mise à jour). Dérivée de X-500 (mais plus simple que cette dernière), cette norme est utilisée pour rédiger des répertoires d'adresses ou de numéros de téléphone. Il s'agit d'un service plutôt orienté vers les grosses bases de données et les répertoires de grosses entreprises, et il ne peut probablement pas remplacer le carnet d'adresses dont presque tout utilisateur de courrier électronique dispose dans son logiciel de messagerie.

La définition provient des RFC 1777 et 1778.

Légende urbaine

Un type particulier de rumeur qui est sociologiquement marqué par une propagation « naturelle » favorisée par un type de crainte de la technologie ou d'une technologie mal comprise. Par exemple, les rumeurs sur l'existence de virus absolument terribles relèvent généralement de la légende urbaine, à cause de la méconnaissance commune des mécanismes exacts de la propagation des virus.

Voir aussi « appels ».

LetterBounce

Un utilitaire assez simple qui permet de faciliter une tâche ingrate du gestionnaire d'une (ou plusieurs) liste(s) de messagerie. Très régulièrement des courrier distribués par la liste de messagerie sont retournés avec un message d'erreur. Le traitement habituel est de retirer l'adresse en cause de la liste.

LetterBounce reçoit les retours en erreur, les décode et envoit automatiquement les demandes de désabonnement au gestionnaire de liste. Très appréciable si vous gérez une grosse liste de messagerie ou si vous gérez plusieurs listes simultanément.

Lettres d'amour

Le courrier électronique en se développant est devenu un média comme beaucoup d'autres. Aujourd'hui, de nombreuses histoires d'amour se sont nouées autour du courrier électronique ou qui se sont développées en utilisant le courrier électronique comme moyen de rester en contact lorsque l'on est à distance.

Listbot

Robot logiciel qui gère une ou plusieurs listes de messagerie (gestionnaire de liste de messagerie).

Liste de diffusion

Ce terme est employé dans deux contextes proches. Soit, il s'agit d'un équivalent de « liste de messagerie ». Soit, dans un logiciel de messagerie électronique, on trouve ce terme pour désigner une fonctionnalité, extension du carnet d'adresses, qui permet d'envoyer un même message à plusieurs adresses de courrier électronique (à plusieurs destinataires inscrits dans la liste de diffusion).

Liste de messagerie

Afin de permettre de partager une conversation par courrier électronique entre davantage de personnes qu'un seul expéditeur et un seul destinataire il a été inventé plusieurs techniques. Celle de la liste de messagerie fournit une adresse e-mail particulière qui sert de relais pour la distribution de courrier à un groupe de participants. Tout le monde écrit à la même adresse (par exemple, liste-des-copains-de-Pierre@gestion.mail.com). Chacun des participants reçoit une copie du courrier.

Un livre conseillé :

Managing Mailing Lists Majordomo, LISTSERV, Listproc, and SmartList

d'Alan Schwartz

1st Edition March 1998

Editions O'Reilly

1-56592-259-X, 296 pages

La liste de messagerie est plus souple que l'emploi de Cc: et Bcc: parce que seul un gestionnaire de la liste a à tenir compte des aspects de gestion (ajouts, retraits, etc.). On dit que le gestionnaire ou administrateur s'occupe de la gestion des abonnements à la liste. Cet aspect est central dans les listes qui contiennent un nombre important de participants qui ne se connaissent pas forcément (dans notre exemple, Pierre sait quelle est la liste de tous ses copains – ou de tous ses fans, mais ils ne se connaissent pas nécessairement et ne souhaitent pas forcément être connus).

On utilise des listes de messagerie pour toutes sortes d'application parmi lesquelles on comptera la distribution de journaux ou lettres d'information, la communication d'une entreprise avec ses clients, la coordination d'association ou de groupes d'utilisateurs, etc.

Il existe des logiciels spécialisés dans le gestion de listes de messagerie et certains logiciels de serveurs de courrier électronique (comme Mercury de David Harris) incluent aussi cette fonctionnalité.

Listes de télémarketing

En relation directe avec le SPAM, on entend beaucoup parler de listes des télémarketing. Ce sont ces listes d'adresses qui sont utilisées par les sociétés qui font du télémarketing.

Certaines sont parfaitement légitimes : elles ont été constituées par des sociétés ou des sites web en demandant leur adresse à leurs visiteurs et en indiquant clairement à quel usage elles sont destinées.

Certaines sont seulement vaguement légitimes (et totalement illégales en France grâce à la CNIL) : elles été constituées par des sociétés ou des sites web en demandant leur adresse à leurs visiteurs mais en dissimulant leur usage véritable (par exemple, en cachant qu'elles seraient utilisées par d'autres sociétés).

Certaines sont totalement intolérables : elles ont été constituées par tous moyens (y compris le ramassage d'adresses dans les sites wbe ou les groupes de discussion de Usenet).

On pourra rajouter que certaines listes sont le fruit du rachat d'autres listes. Ainsi, certaines sociétés - insuffisament soigneuses ou attentives - achètent les listes de spammeurs et se rerouvent directement classées comme telles. A mon avis, les entreprises qui veulent ainsi acheter des listes d'adresses ont intérêt à procéder avec le plus grnad soin. Au minimum, je leur conseillerai de contrôler le contenu exact de la déclaration faite à la CNIL pour la liste qu'elles souhaitent acheter. Si la déclaration ne faisait pas état de la possibilité de revendre la liste, le risque légal est non-négligeable. Si la délcaration n'était pas accompagnée d'une notice claire sur le site web qui a fait la collecte, le risque est décuplé. Si la liste est ancienne, les personnes qui y sont inscrites ne le savent plus et les mails inattendus seront classés comme du SPAM. La réputation d'une entreprise peut être rapidement ternie de manière indélébile par un responsable marketing « trop rapide » dans ce genre de processus de sélection.

Liste noire

Dans le cadre de la lutte contre certaines pratiques sur Internet, il arrive que soit utilisé un outil particulier le plus souvent appelé « liste noire » et qui regroupe les moutons noirs identifiés selon certains critères spécifiyues à la liste. Par exemple, une liste noire de spammeurs va lister ces individus ou ces domaines. L'implication portée par l'adjectif « noire » est que la liste regroupe selon un critère négatif (qui peut être le SPAM comme dans notre exemple, l'existence d'un open relay comme pour les RBL, ou autre).

Voir aussi RBL, SpamAnti.net et une comparaison assez extensive de tous les fournisseurs de listes noires d'adresses IP : http://www.sdsc.edu/~jeff/spam/cbc.html

listserv et listproc

Ces deux outils sont des gestionnaires de listes de messagerie largement reconnus. Ils sont distribués respectivement par L-SOFT et par CREN.

Logiciels de SPAM

Si vous êtes venu ici pour en trouver une liste, je regrette de vous informer que j'ai volontairement décidé de ne faire apparaître aucun nom, ni aucune adresse susceptible d'aider un spammeur amateur.

Il est exact que certains logiciels sont spécialement consacrés à la pratique du SPAM. Il s'agit de logiciels de courrier électronique légèrement modifiés afin de faciliter le travail d'un spammeur. Ils incluent souvent des informations fausses ou trompeuses dans le courrier pour compliquer la vie des chasseurs de spammeurs. Ils procurent certaines aides pour le camouflage.

Toutefois, sans donner de noms, il est clair que la grande majorité des produits proposés sous cette étiquette sur Internet ne valent même pas l'effort de les downloader. Sans parler de les payer. Néanmoins, quelques uns d'entre eux sont de véritables plaies pour la communauté anti-SPAM.

Il suffit de finir en disant que l'emploi du mauvais logiciel lors de la première campagne de SPAM par un marketing trop content d'avoir trouvée la panacée peut se traduire par une chasse réussie, l'identification du spammeur en quelques heures et son inscription définitive dans les dizaines de listes noires qui existent sur Internet...

Loop

Voir « boucle ».

Loopback

Pour assurer certains tests de bon fonctionnement du courrier électronique, il est fait usage d'une adresse particulière (loopback) qui a pour rôle de retourner automatiquement à l'envoyeur les courriers électroniques qui lui sont adressés.

Plus particulièrement, le RFC 1911 (« Voice profile for Internet mail ») impose l'existence de ce type d'adresse pour tous les domaines. Toutefois, cela reste loin d'être une réalité courante.

Certains domaines ont publié l'existence de leur propre adresse de loopback :

Adresse	*Remarques*
echo@seattlelab.com	
test-courrier@sogi.com	En français
echo@telcomplus.net	La réponse (en anglais) la plus courte
test@alphanet.ch	En anglais, mais avec une réponse qui comporte pas mal d'éléments (pas tous très sérieux)
echo@tu-berlin.de	En allemand
test@mega.bw	
internet@gurus.com	
ping@stamper.itconsult.co.uk	
echo@tu-chemnitz.de	
loopback@bristol.com	Cette adresse (quand elle fonctionnait encore) était gérée par le script qui est reproduit au paragraphe « Code de loopback ».
echo@bvrpusa.com	

Si vous connaissez d'autres adresses (publiques) de ce type, merci de me les signaler directement pour inclusion dans une future version de cette petite encyclopédie.

Note : on remarquera le site www.GetResponse.com qui permet de créer facilement une adresse à réponse automatique.

Loser

Traduction française : perdant (mais avec la connotation qui provient de l'assonnance avec user (utilisateur, en anglais)).

Voir aussi luser.

Lotus Notes

Ce produit très complet de gestion de la communication interne d'entreprise et de collaboration d'entreprise comprend une messagerie assez complète et compatible avec le courrier électronique Internet.

Lotus Notes a été racheté en 2000 par IBM chez qui le logiciel continue une carrière qui continue à préserver une certaine autonomie dans la grande maison d'Armonk malgré les craintes initiales des plus fervents partisans de ce logiciel qui pensaient que le géant bleu absorberait et détruirait Lotus dans un ultime baiser de la mort.

http://www.lotus.com/

Un livre conseillé :

Lotus Domino Administration in a Nutshell

De Greg Neilson

Août 2000

Editions O'Reilly

1-56592-717-6, 368 pages

Luser

Contraction de Looser (perdant) et de User (utilisateur). Désigne un utilisateur particulièrement stupide, ou dangereux, ou engagé dans des activités qui causeront bientôt (ou ont déjà causé) sa perte.

Voir aussi loser.

Lyris

Le nom d'une société (et de sa ligne de produits) qui s'est spécialisée dans les outils de gestion du courrier électronique. Ils ont longtemps été les seuls à supporter listserv (maintenant ListManager) comme serveur de liste de messagerie. Ils effectuent également de l'hébergement de listes de messagerie pour les entreprises et ils proposent un produit de filtrage des courriers électroniques : MailShield.

http://www.lyris.com/

3.14. M

MailShield

Un logiciel de filtrage de courrier électronique très complet et très configurable. Il n'est pas toujours facile d'organiser le filtrage des courriers électronique sans connaissances en programmation ; MailShield apporte une solution à ce problème de certains administrateurs de courrier électronique.

Mallet

En français, « Maillet ». Un objet contondant qui est utilisé de manière métaphorique pour punir violemment un utilisateur particulièrement stupide ou dangereux. De manière compréhensible, l'usage de ce terme est rarissime parmi les utilisateurs alors qu'il peut se rencontrer plus facilement parmi les administrateurs de systèmes ou de réseaux.

Voir aussi LART et Golden Mallet.

MAPI

Mail Application Programming Interface.

Interface propriétaire (Microsoft) pour accéder à des logiciels clients de messagerie.

Mailbombing

Terme anglais qui décrit l'action de « bombarder » quelqu'un avec des messages de courrier électronique. Cela entre dans la catégorie plus générale des dénis de service, puisque ce type d'attaque consiste à envoyer un tel nombre de messages que le destinataire en est incommodé (et probablement incapable d'utiliser sa messagerie électronique).

Mailbot

Robot logiciel qui effectue des opérations automatiques de courrier électronique (envoi automatique, réponse automatique, etc.)

Par exemple, on parlera de mailbot pour les logiciels qui sont capables de répondre à vos correspondants quand vous recevez un courrier électronique pendant vos vacances.

Mailer:

Un en-tête non standard indiquant le type de logiciel de messagerie de l'expéditeur.

MailExpire

Un service qui propose des adresses de courrier électronique « jetables » pour gérer les risques de SPAM.

http://www.mailexpire.com/

Mailing list

Voir liste de messagerie.

Mail Marshal

Un assistant de filtrage et un serveur de messagerie qui fonctionne sous Windows 2000/NT. Il peut être accompagné d'un anti-virus pour détecter les virus en plus des SPAMs.

http://www.messagingsolutions.com/MailMarshal.htm

Mailing-List:

Certains logiciels de gestion de listes de messagerie insèrent cet en-tête dans le corps des messages qu'ils envoient.

Exemple :

Mailing-List: contact users-help@openoffice.org; run by ezmlm

Mail warden

Un logiciel de BVRP Software qui assure une fonction de filtrage du courrier électronique pour un serveur Domino (Lotus Notes) ou SMTP. Il protège contre les virus, les vers et le SPAM selon les dires de son concepteur.

MailShell

Un système de filtrage qui cherche à éviter que le SPAM n'arrive dans votre boite-à-lettres. Entre autres choses, il utilise des adresses temporaires et jetables. Service payant.

http://www.mailshell.com/

Mail Siphon

Outre ses fonctions permettant de déboucher aisément une boîte-à-lettres obstruée par d'énormes messages, Mail Siphon II est un véritable agent de courrier élecronique (réception et envoi).

Mail Siphon II permet d'accéder depuis un Macintosh à ses différentes boîtes aux lettres, de lire les messages présents, d'y répondre ou de les effacer.

http://www.maliasoft.com/siphon/index_fr.html

Mail-System-Version:

Un en-tête non standard indiquant le type de logiciel de messagerie de l'expéditeur.

mailx

Un logiciel client de gestion de courrier éelctronique développé par l'Université de Californie à Berkeley (UCB). Il est orienté texte et géré ligne-à-ligne, ce qui en fait un ancêtre un peu difficile à utiliser.

majordomo

Un gestionnaire de listes de messagerie principalement utilisé sur des serveurs Unix ou GNU/Linux.

Mail Abuse Prevention System (MAPS)

Cette association américaine essaye de traiter le prblème du SPAM par des actions de sensibilisation et d'information auprès des gestionnaires de courrier électronique. Leur outil principal est un ensemble de conseils permettant de rédiger des règles d'usage limitant les utilisateurs afin d'éviter la production de SPAM.

http://mail-abuse.org/

Initialement, cette association était une activité de Vixie Enterprises de Paul Vixie.

Marketing direct

Ce terme regroupe de nombreuses techniques de marketing qui essayent de cibler très précisément les clients concernés et de les contacter le plus directement possible. On y trouve le démarchage téléphonique, le démarchage par courrier électronique, etc. Le démarchage par courrier électronique connait une version particulièrement visible sur Internet : le SPAM ou courrier électronique non sollicité. On comprendra donc que le démarchage par courrier électronique n'est pas toujours du SPAM : un démarchage auprès d'une cible de clientèle qui a donné son accord pour être contacté par ce moyen est considéré comme licite même par les opposants au SPAM.

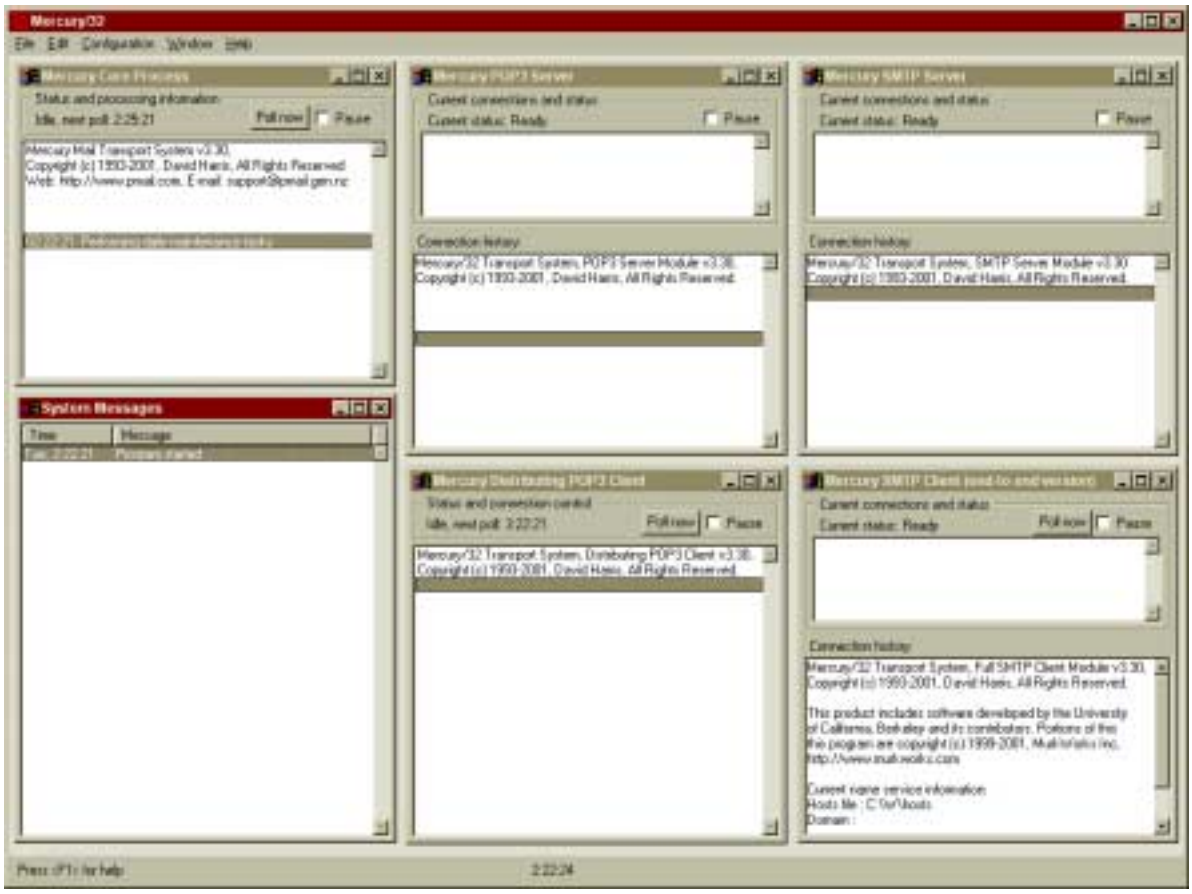
On remarquera quand même que s'il s'écoule un temps important entre l'autorisation préalable et le démarchage, les réactions des destinataires peuvent être négatives du fait d'un certain « oubli » de l'utilisateur. Je conseille donc aux gestionnaires de listes de messagerie de toujorus prévoir l'envoi d'une lettre d'information par mois au minimum pour s'assurer qu'ils sont toujours « connus » de leurs abonnés. Cela évite des tas de petits problèmes.

Menaces de mort

Certains semblent oublier un peu facilement que le courrier électronique est un moyen hors de portée du droit tradionnel. Cela a parfois mené à la rédaction de menaces de mort de la part de personnes, excédées sans doute. Toutefois, il est important de rester conscient que le moyen ne change rien à la gravité de ce genre de menaces (de même que pour les actes qui relèvent du chantage, de la diffamation ou d'autres actes répréhensibles).

L'age de certains internautes explique partiellement certains comportements, mais ne les excuse pas aux yeux de la justice.

Mercury



Logiciel gratuit (freeware) de gestion de courrier électronique écrit par David Harris. Il permet de constituer un MTA ou Mail Transfer Agent et un serveur de messagerie très complet sur un PC sous Windows (contient également un gestionnaire de liste de messagerie).

http://www.pmail.com/

Message en clair signé

Nom anglais original : clear-signed message.

Un message électronique signé par S/MIME ou PGP mais dont le contenu est clairement lisible même si la signature ne l'est pas.

Message-ID:

Cet en-tête contient un identifiant réputé unique pour le message. La forme est relativement libre, mais un exemple serait :

Message-ID: <000601c187dc$0f401f60$0201a8c0@Cyrene>

Il est important de comprendre que, malgré l'aspect parfois compréhensible de la valeur présentée, il n'y a pas de forme garantie. Et il est donc particulièrement risqué d'essayer de tirer des conclusions à partir de ce seul en-tête.

Par convention (mais il y a quelques exceptions), cet en-tête est de la forme « illisible@serveurMTA.USA.net », où « serveurMTA.USA.net » est le nom de la machine qui a rempli ce

champ et la partie « illisible » est en fait une chaîne plus ou moins unique qui contient parfois le nom de l'utilisateur (voir l'exemple ci-dessus).

Messagerie électronique

Terme un peu générique habituellement employé pour décrire l'ensemble des services de gestion du courrier électronique. Parfois, simplement employé comme substitut de ou équivalent à *courrier électronique*.

Messenger

Logiciel de messagerie électronique de Netscape. Il est généralement livré en compagnie de Netscape Navigator dans le produit Netscape Communicator.

http://www.nestcape.com/

metamail

Un ensemble d'outils qui permettent de faciliter la configuration de logiciels de gestion de courrier électronique. Il a d'abord été développé par Bellcore, mais il est disponible gratuitement. Honnêtement, c'est un outil pour programmeur, pas pour un utilisateur lambda.

mh

Un ensemble d'outils qui, mis ensemble, constituent un logiciel client de gestion de courrier électronique. Il a d'abord été développé par Rand Corporation, puis supporté par l'Université de Californie à Irvine. Rustique, mais il continue à évoluer de nos jours (par exemple, MIME a été implémenté dans mh).

MHTML

MIME-enhanced HTML.

Une extension de MIME qui permet d'envoyer des documents complexe HTML (y compris avec des images) dans des messages de courrier électronique sous la forme d'un seul message MIME.

Microsoft

L'incontournable leader mondial du logiciel. Producteur d'Outlook, Outlook Express et Exchange (pour ne citer que ceux-là).

MIME

Afin de faciliter le transport de fichiers binaires, il est souhaitable de les « convertir » en ASCII. Le format MIME est actuellement celui qui l'emporte parmi toutes les méthodes proposées. Il est en train de devenir le standard de fait.

Le codage MIME, très complet, est décrit principalement par le RFC 2045.

MIMEsweeper

Un logiciel (provenant de Baltimore Technologies Plc.) pour serveur de messagerie capable de traiter automatiquement le courrier électronique en vue de fournir des services du type filtrage de SPAM, filtrage de contenus considérés comme indaptés, détection des virus à l'entrée ou à la sortie, compléments automatiques sur les courriers sortants (comme de toujours rajouter une mention de non-responsabilité sur tous les courriers électroniques d'une entreprise).

http://www.baltimore.com/

MIME-Version:

Cet en-tête décrit le type de codage MIME qui est employé dans le message. Cela permet d'éviter des confusions tout en autorisant l'évolution du standard. La forme exacte de cet en-tête est très flexible tout en étant formellement décrite par le RFC 822. En particulier un commentaire (au sens du RFC 822) peut être introduit à n'importe quel endroti de la chaîne comme dans les cas suivants qui sont exactement équivalents :

MIME-Version: 1.0
MIME-Version: 1.0 (produced by MetaSend Vx.x)
MIME-Version: (produced by MetaSend Vx.x) 1.0
MIME-Version: 1.(produced by MetaSend Vx.x)0

MLM

Multi-Level Marketing.

Une des sous-catégories de SPAM assurant pouvoir dévoiler une méthode pour gagner de l'argent rapidement. Contrairement à ce qui est parfois dit par les spammeurs, ces techniques et les arnaques pyramidales, consistent à faire comercialiser un produit par un nombre important d'intervenants. Les gains de chacun sont généralement proportionnels aux ventes réalisées par soi-même (et par les autres personnes qu'on a « parrainnées »). Les ventes organisées par Tupperware dans les années 70 relevaient de ce type d'organisation. Elles se sont révélées ne rappporter que de petites sommes.

Les arnaques pyramidales ajoutent à l'approche MLM une garantie de gain qui en fait repose uniquement sur l'apport de nouvelles victimes. Toutefois, ces arnaques s'écroulent systématiquement au moment de la saturation.

Si le Multi-Level Marketing est souvent toléré par la Loi, il est fermement encadré. Et il y a peu d'endroits dans le monde où les arnaques pyramidales ne sont pas l'objet d'une répression très stricte (souvent à la suite d'incidents majeurs qui peuvent avoir « ruiné » de très grand nombres de gens).

MMF

Make Money Fast.

Le type particulier de SPAM qui fait la promotion de méthodes permettant de gagner beaucoup d'argent en peu de temps (une des sources majeures de SPAM). Cela relève plus de l'escroquerie que de quoi que ce soit d'autre. Nombre des solutions proposées sont considérées comme purement et simplement illégales dans de nombreux pays.

MOSS

MIME Object Security Services.

Un protocole d'échange de messages e-mail signés et/ou cryptés. N'a pas eu un grand succés.

Mot de passe (ou password)

Dans de nombreux processus d'authentification, il est utilisé un mot de passe qui est un mot (ou un groupe de caractères ou de chiffres) que seul l'utilisateur est censé connaître.

La plupart des protocoles de courrier électronique (comme POP3) utilisent aussi des mots de passe comme moyen d'authentification des utilisateurs. Une des faiblesses reconnues de SMTP est de ne pas facilement permettre cette authentification par mot de passe. On utilise alors souvent l'association de POP3 et de SMTP pour contourner le problème.

Moteur de recherche

Les auteurs ou propriétaires de sites web sont très sensibles à leur classement dans le plus grand nombre possible de moteurs de recherche. Cela les pousse à s'inscrire sur les moteurs les plus connus. Après un certain temps (parfois très court) ils découvrent les sites ou les services qui promettent de les inscrire sur des dizaines, des centaines ou des milliers de moteurs de recherche.

Halte là ! Le SPAM est là.

En effet, ces services proposent des inscriptions sur des sites qui n'ont de moteur de recherche que le nom. Le plus souvent (en plus de quelques moteurs de recherche parfaitement légitimes et intéressants ou utiles), il s'agit de systèmes de petites annonces croisées qui ne présentent aucun intérêt. Pire encore ! Ils sont le plus souvent associés à des services de publicité par courrier électronique (comprenez du « SPAM »).

Et oui, l'usage de ces services se traduit par un véritable déluge de SPAM dans les minutes qui suivent le début de l'inscription. Il n'est pas anormal de recevoir littéralement des *milliers* de SPAM en quelques minutes. Et ensuite, l'adresse de courrier électronique que vous aviez imprudemment utilisée est inscrite sur des centaines de listes de spammeurs. Elle sera revendue pendant des années. Considérez donc là comme perdue.

Quels conseils vous donner ? Il y en a trois à mon avis.

A/ Vous connaissez déjà les noms des moteurs de recherche utiles ou bien ils sont inutiles. Vous pouvez donc perdre une dizaine de minute pour vous *inscrire manuellement* chez Google, Altavista, Yahoo, Lycos et quelques autres. De toutes manières, un certain nombre d'entre eux ne permettent plus l'inscription automatique (voir la technique de code à entrer manuellement dans Altavista).

B/ Le *nombre de moteurs de recherche* ne compte pratiquement pas. Seuls quelques uns peuvent vous apporter du trafic. Les autres ne sont que poudre aux yeux en terme d'utilité et de nombre de visite. Tous les gestionnaires de site web vous le confirmeront.

C/ Si vous voulez quand même tenter votre chance (c'est risqué mais tant pis pour vous), il faut absolument utiliser une *adresse de courrier électronique strictement jetable*. Je conseille de créer une adresse chez un hébergeur gratuit (ne vous préoccupez pas de lui donner un nom utile). Ensuite, utilisez exclusivement cette adresse jetable pour les inscriptions automatiques. Les SPAMs tomberont dans une boîte-à-lettres que personne ne consultera jamais. Ou alors utilisez une fausse adresse (soyez certain qu'elle n'est pas utilisée par quelqu'un). N'utilisez jamais une adresse sur un domaine qui existe (même example.net qui est réservé - voir l'article correspondant).

Dans le cas où vous insistez pour utiliser ces services, n'oubliez pas que vous tendez des batons pour vous faire battre. Les aspirateurs d'adresses des spammeurs sont là intéressés par la seule adresse de votre site web (où ils escomptent retrouver vos adresses de courrier électronique).

Comme partout ailleurs, il n'y a pas de recette miracle. Vous devriez l'avoir déjà compris si vous lisez cette encyclopédie depuis la première page...

MTA

Mail Transfer Agent.

Un agent (un logiciel) opérant sur le courrier électronique et dont le rôle est de transférer ou déplacer du courrier d'une machine à une autre, d'un service à un autre. Le terme est alors équivalent en français à « passerelle de messagerie ».

Parfois, le terme MTA désigne plus simplement un serveur qui utilise le protocole SMTP.

MUA

Mail User Agent.

Terme équivalent en français à « Client de messagerie ».

Murkowski

Sénateur américain célèbre pour avoir proposé en 1997 une législation extrêmement favorable aux spammeurs. Elle n'a pas été votée et reste donc (heureusement) lettre morte.

Contrairement à ce que disent les dernières lignes de nombreux SPAM, il n'y a pas actuellement de législation fédérale américaine concernant le SPAM. Le sénateur Frank Murkowski avait ouvert une boite-à-lettres électronique de commentaires (commercialemail@murkowski.senate.gov, maintenant fermée) qui le confirme dans la réponse automatique renvoyée à tous ses correspondants (« la 105e session du Congrès a ajourné ses travaux sans voter de nouvelle loi sur ce sujet. Actuellement, il n'y a pas de loi fédérale qui réglemente le "junk mail" »).

http://davearonson.home.att.net/spammurk.html

Voir aussi le chapitre sur la législation à la fin de ce document.

MX record ou enregistrement MX

Le terme français (« enregistrement MX ») est rarement utilisé. Mail Exchange record.

Information qui fait partie des enregistrements fournis par le protocole DNS qui permet de construire une route pour accéder à un domaine. Selon l'endroit où se trouve un domaine sur Internet, le chemin d'accès est plus ou moins simple. Les agents de transfert de courrier électronique sont obligés de déterminer une route (éventuellement directe) pour pouvoir livrer le courrier électronique à cette destination. Un nom de domaine peut avoir plusieurs routes qui sont éventuellement fonction de l'origine du courrier électronique et de la priorité du message. Chaque route peut avoir une ou plusieurs options de routage en sauvegarde (en cas de défaillance d'une route principale).

Le MX record est une des ressources accessibles par l'intermédiaire du protocole DNS et intéressantes à plusieurs titres pour les serveurs de messagerie.

3.15. N

NANAE

news.admin.net-abuse.email.

Une hiérachie Usenet dans laquelle sont traités de nombreux problèmes d'abus du courrier électronique (dont le SPAM). Le point de ralliement d'une grande partie de la communauté anti-SPAM. La longueur du nom du groupe de discussion en rend l'usage difficile, ce qui explique la création de ce raccourci très conforme aux habitudes de Usenet. Mais étant donné l'intérêt très particulier de ce groupe de discussion, l'emploi du raccourci « NANAE » ou « nanae » est quasiment devenu un signe de reconnaissance pour la communauté anti-SPAM (à peu près les seules personnes qui peuvent savoir ce que cela signifie).

Ce groupe de discussion où 90% du trafic a lieu en anglais, accueille aussi bien des dénonciations de spammeurs que des discussions sur les moyens de reconnaître l'origine d'un SPAM, sur les moyens légaux de réduire le problème, sur la meilleure manière de configurer un serveur de messagerie. Toutefois, il s'agit d'un groupe avec un volume de participation inhabituellement élevé, avec un bruit de

fond important, un niveau technique difficile et une agressivité latente rapidement perceptible (les erreurs des uns ou des autres sont accueillies sans tendresse ni patience).

NANAS

news.admin.net-abuse.sightings.

Un groupe de discussion Usenet sur lequel on rencontre peu de discussions (elles ont plutôt lieu sur le groupe voisin new.admin.net-abuse.email), mais où les utilisateurs publient les incidents de type abus (les SPAMs par exemple). Certains combattants du SPAM utilisent ainsi ce groupe de discussion pour alimenter leurs listes noires ou pour faire des statistiques sur les types d'abus rencontrés couramment.

Nétiquette ou netiquette

Ensemble informel de règles de savoir-vivre et de bonne conduite sur Internet et dans l'usage du courrier électronique. Le terme (pratiquement identique en anglais et en français) est une contraction de « net » (réseau en anglais) et d'étiquette (au sens où on l'entendait à la cour du Roi Soleil). Il existe sur Internet quelques documents qui essayent de rassembler en un corpus « législatif » homogène ce qui n'est souvent que la formalisation d'un consensus social par définition imprècis et mouvant. Mais le non-respect de ces règles - comme dans toute société - expose les contrevenants à l'ire de leurs pairs et à l'opprobe sociale. Si les infractions à la nétiquette sont aujourd'hui plus tolérées que dans les jeunes années d'Internet, elles constituent maintenant davantage un moyen de reconnaissance sociale pour des groupes qui se distinguent par leurs pratiques et leurs tolérances différentes en matière d'usages et de règles de vie autour du courrier électronique (les vieux hackers, les jeunes hackers, les internautes récents, etc.)

Newsgroups:

Un en-tête qui n'apparaît qu'en cas de courrier électronique en relation avec un envoi (*post*) sur un groupe de discussion Usenet (copie courrier d'un envoi, réponse e-mail à un envoi Usenet). Il indique le nom du groupe de discussion dans lequel se tient la discussion à laquelle le message participe. Il existe deux syntaxes distinctes.

Nigéria et arnaque nigériane

Arnaque financière connue antérieurement à l'apparition d'Internet, mais qui a maintenant pris une ampleur particulière par l'emploi du SPAM pour se diffuser.

Dans la pratique, les courriers sont annoncés comme provenant du Nigéria aussi bien que de l'Angola, l'Afrique du Sud, le Sierra Leone, le Zimbabwe, etc. même s'il s'agit d'escroqueries qui n'ont pas grand rappport avec l'un de ces pays.

Le gouvernement nigérian (et la Special Force Unit – SFU – de la Police) est même suffisament concerné par la situation pour essayer de mettre un terme à cette association peu appréciable entre leur pays et une vague continue d'escroqeries. Par exemple, début 2001, il y a eu une série de 300 arrestations qui a mené à 25 inculpations. On parle même d'arnaque 419 en faisant référence à la section applicable dans le code nigérian de la criminalité.

Voir l'article « Kabila » et le site www.scamorama.com qui comporte à peu près toutes les variations connues de cette arnaque.

NNTP

Le protocole IP utilisé par les groupes de discussion Usenet.

Nom de domaine

L'adresse ou le nom d'une famille de machines. Il s'agit également de la partie de l'adresse de courrier électronique qui se trouve à droite du signe @.

Longtemps limité à 22 caractères, puis le suffixe dit « de TLD », le nom de domaine peut aujourd'hui atteindre 63 caractères.

Notes

Voir Lotus Notes.

nPOP

Un tout petit logiciel de messagerie. A mon avis un peu court, pour la plupart des utilisateurs, mais il a ses adeptes. Le code source est disponible (à l'origine il était prévu pour tourner sur Pocket PC), il est infiniment plus facile à utiliser que bien d'autres logiciels. A considérer.

http://www.nakka.com/soft/npop/index_eng.html

Nuke

Abbréviation anglo-américaine de « nucléaire » ou de « bombe nucléaire ». Verbe employé pour décrire l'action qui consiste à détruire définitivement quelque chose (souvent employé quand on ferme le compte d'un utilisateur en sanction après un abus, à cause de la connotation violente et sans appel associé à l'arme nucléaire) : « to nuke the user account (*détruire le compte utilisateur*) ».

Du fait de son efficacité et de sa simplicité, le terme est aussi utilisé par des administrateurs francophones.

Numéris

Il s'agit de la marque utilisée par France Télécom pour distribuer la technologie ISDN ou RNIS à ses clients.

3.16. O

Obsoletes:

En-tête non standard ou Usenet qui désigne la référence d'un article ou d'un message de courrier électronique précédent qui est remplacé par celui-ci. En dehors du contexte Usenet, peu de logiciels de messagerie reconnaissent cet en-tête (même dans le contexte X.400).

Voir aussi Supersedes:.

Off-topic

Voir « hors sujet ».

Open relay

En français « relais ouvert ». La traduction française n'est pratiquement jamais employée.

Voir relais.

Opt-in

Notion centrale dans la lutte contre le SPAM. L'opt-in (ou « choix d'entrer ») décrit une méthode adoptée pour rejoindre une liste ou un fichier d'adresses de messagerie. Selon cette méthode, la décision doit être prise consciemment et volontairement par l'utilisateur. Il n'est jamais inscrit d'office (même temporairement).

L'avantage de cette méthode pour l'utilisateur est qu'il ne reçoit pas de courrier électronique qu'il n'a pas choisi de recevoir. Elle a donc la faveur de la plupart des opposants au SPAM (ou courrier électronique non sollicité).

Plus important encore, c'est la méthode légalement imposée depuis mai 2002 par l'Union Européenne pour toutes les communications commerciales par courrier électronique.

Voir aussi opt-out.

Opt-in/opt-out - choix pré-sélectionné ou pas

Il arrive que certaines personnes utilisent (en français) le terme opt-in de manière erronnée. Cela a causé quelque confusion (qui n'existe apparemment pas hors de France - pas même dans les autres pays francophones semble-t-il). Ces personnes devant un formulaire qui propose de s'inscrire sur une liste de messagerie (par exemple, avec l'option « j'accepte que mon adresse soit transmises à des tiers ») disent opt-out si la case est cochée préalablement ou opt-in si la case n'est pas cochée à l'arrivée du visiteur.

J'indique cette acception parce qu'elle existe (je l'ai rencontrée plusieurs fois), mais je la déconseille très vivement parce qu'il s'agit d'un très mauvais exemple de franglais extrême (un mot anglais, avec un sens technique propre, est repris dans un sens très différent mais susceptible d'induire en erreur par un jeu de « faux-ami »). Dans la pratique, on trouve - parmi les gens qui ne maîtrisent pas bien la notion - un certain nombre de spammeurs impénitents qui tentent de contourner leurs obligations par une manipulation consciente de la traduction d'une langue dans l'autre.

Opt-in double ou double opt-in ou opt-in confirmé

L'opt-in n'est pas la panacée universelle. Cette approche garantit à peu près que la liste de messagerie n'est pas alimentée avec des adresses qui n'ont pas choisi l'inscription. Mais quelqu'un de mal-intentionné peut inscrire une adresse sans le consentement de son véritable propriétaire. Il peut s'agir d'un plaisantin qui va inscrire quelqu'un sur des dizaines de listes de messagerie (rendant la vie impossible à la victime) ou d'un ingénieur marketing peu scrupuleux qui va utiliser le formulaire d'inscription pour inscrire tous ses prospects (et pourra ensuite se rétracter derrière un mensonge du type « l'inscription a bien eu lieu sur notre site tel jour à telle heure... Nous ne pouvions pas savoir que ce n'était pas vous qui le demandiez »).

Pour se protéger, la plupart des logiciels gestionnaires de messagerie proposent une option de double opt-in ou de confirmation d'inscription. Quand une adresse est inscrite, un message de demande de confirmation lui est immédiatement envoyé. L'inscription n'est effective que si le destinataire répond à ce message (qui contient généralement un code unique de confirmation). En l'absence de réponse de confirmation, l'adresse est simplement oubliée ou abandonnée.

Je conseille vivement à tout gestionnaire de liste de messagerie de prévoir cette option dès l'origine. Elle évite les contestations désagréables. Cela laisse une trace de la confirmation dans les enregistrements du gestionnaire de liste, comme ceux du serveur de mesagerie. Cela donne une occasion supplémentaire d'informer techniquement le destinataire. La simplicité de l'opération pour l'utilisateur

(simplement cliquer sur le bouton « répondre » sans rien changer au message de demande de confirmation) garantit un excellent taux de réussite.

Opt-out

Par opposition à opt-in, l'opt-out (ou « choix de sortir ») décrit une méthode adoptée pour rejoindr une liste ou un fichier d'adresses de messagerie. Selon cette méthode, l'utilisateur peut être inscrit sur la liste sans le savoir ou sans en être informé. Mais il a la possibilité de demander à être retiré de la liste.

Cette méthode a la faveur de nombreux partisans du marketing électronique (et de nombreux spammeurs) parce qu'elle permet de concevoir des « campagnes » de promotion qui n'utilisent que peu de ressources en amont (uniquement l'achat de fichiers) et supposent que les destinataires se contenteront d'ignorer les courriers qu'ils recoivent mais ne les intéressent pas. La proximité de principe avec la situation du courrier postal traditionnel (sur laquelle insistent ses partisants) est souvent contestée par les opposants au SPAM qui font remarquer que cela est le mode de fonctionnement actuel du SPAM qui a démontré sont incapacité à limiter le nombre de courriers indésirables dans les boîtes-à-lettres des utilisateurs.

Opt-in et opt-out sont au cœur de la plupart des législations (ou de leurs discussions) concernant le courrier électronique.

Voir aussi opt-in.

Organization:

Cet en-tête est particulièrement courant, mais n'apporte que rarement une information réellement utile (c'est pourquoi il n'apparaît que rarement dans les en-têtes afichés par défaut). Il indique le nom de l'entreprise, de l'association, de l'organisation, etc. à laquelle appartient l'expéditeur du courrier électronique. On y précise parfois l'adresse d'un site web (entre parenthèses sans que cela ne soit généralement considéré comme de la publicité ou du SPAM).

Exemple :

Organization: Conseil européen de lutte contre le SPAM

Comme l'information qui apparaît là est remplie par l'utilisateur du logiciel lors de son installation, cette information ne peut pas être considérée comme très fiable. Par contre, certains utilisateurs n'hésitent pas à inscrire des textes humoristiques dans ce « champ ».

Original-Encoded-Information-Types:

Liste les types d'encodages utilisés dans le message. RFC 1327.

Originating-Client:

Un en-tête non standard indiquant le type de logiciel de messagerie de l'expéditeur.

Outlook

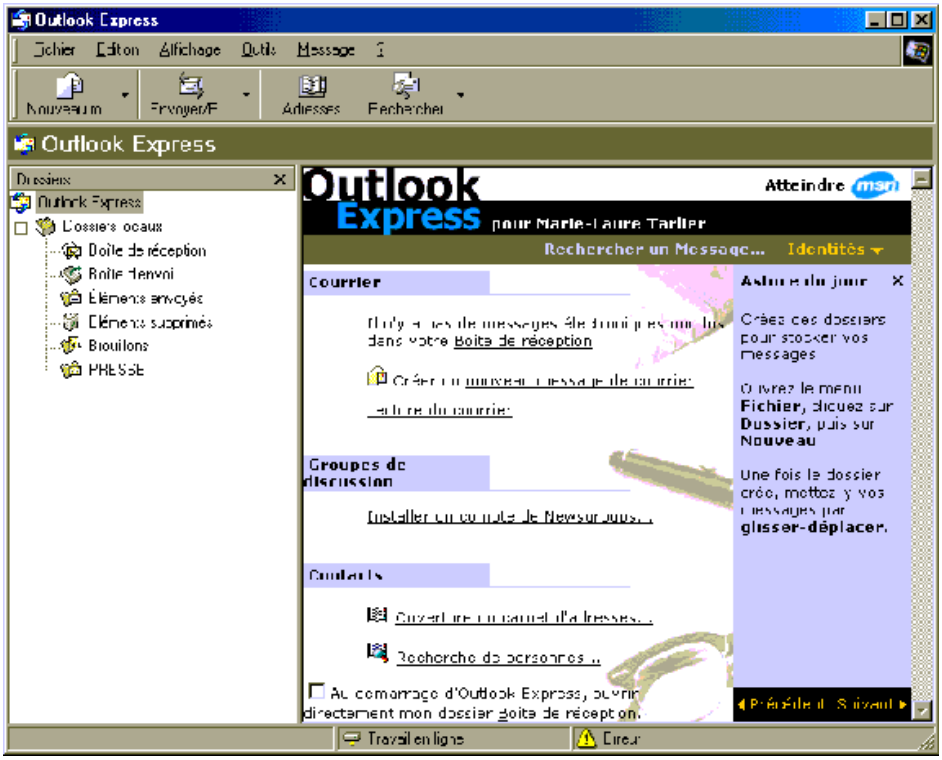
Logiciel de courrier électronique professionnel de Microsoft.

Une caractéristique technique inhabituelle de ce logiciel est le fait qu'il stocke toutes les informations dans un seul fichier qui n'a pas une structure simple et qui peut prendre des proportions considérables (il contient tous les messsages non détruits, des attachements, le carnet d'adresses, etc.) Cette caractéristique est souvent éprouvée comme une vraie difficulté lors des sauvegardes et des opérations d'archivage, comme lors du transfert d'un utilisateur de courrier électronique d'un ordinateur à un autre.

Toutefois, certains logiciels supplémentaires développés par des tierces parties offrent un service spécialement adapté à la solution de ces problèmes.

http://www.microsoft.com/

Outlook Express



Logiciel de courrier électronique grand public de Microsoft. Il s'agit d'une version simplifiée d'Outlook[19] (elle est fournie gratuitement avec Windows).

Malgré de très nombreux défauts (dont celui de produire des courriers dans un format HTML légèrement modifié et hors norme, celui d'avoir la réputation méritée d'être excessivement vulnérable aux virus, vers et autres cyber-attaques et celui de ne permettre qu'un filtrage absolument rudimentaire des messages reçus), c'est sans doute le logiciel de courrier électronique le plus répandu au monde actuellement.

http://www.microsoft.com/

3.17. P

Pare-feu

Internet est un lieu où les problèmes de sécurité se sont révélés importants du fait de la nature libre et ouverte des communications qui y circulent. Parmi les moyens développés pour se protéger (ou protéger un ordinateur ou un réseau), il y a le pare-feu. C'est soit un logiciel, soit un équipement dont le rôle est de séparer une ou plusieurs machines d'Internet (pour les protéger d'une intrusion par exemple), tout en autorisant un usage transparent du réseau.

19 Attention, les deux produits ne sont pas compatibles l'un avec l'autre. En particulier, les formats de fichier utilisés ne sont pas du tout interchangeables. Cela a créé un marché pour des utilitaires de conversion et de transfert entre les deux produits.

Dans le cas d'une entreprise, il n'est pas inhabituel de voir un pare-feu interdire l'entrée du réseau de l'entreprise à des intrus, tout en autorisant le personnel à franchir en sortie le pare-feu pour ses activités habituelles (naviguer sur le web, relever du courrier, etc.)

Devant la complexification des services Internet et la variété des menaces potentielles ou avérées, les types de pare-feu se sont largement diversifiés. On notera l'existence de logiciels dit « pare-feu personnels » ou « personnal firewalls » qui permettent de protéger un PC contre certaines agressions venant d'Internet. Dans tous les cas, ces logiciels ne permettent pas totalement de se sentir en confiance (ils peuvent même parfois créer un faux sentiment d'insécurité), doivent être complétés par un apprentissage des règles élémentaires de sécurité et par l'emploi d'un anti-virus. En effet, les auteurs de virus et autres programmes dangereux n'hésitent pas à exploiter les failles les plus subtiles de ces pare-feu pour les contourner (aucun logiciel n'est exempt de bugs ou de défauts).

Passerelle

Traduction en français de « gateway ».

Ordinateur intercalé entre deux réseaux incompatibles ou partiellement compatibles et qui assure le transport et la conversion des messages qui sont échangés à travers lui.

Sur des systèmes propriétaires (comme AOL, ou la messagerie SMS des téléphones GSM), on trouve souvent une passerelle de messagerie qui intervient entre la messagerie propriétaire de l'entreprise et la messagerie Internet définie par des standard publics. De même, une messagerie comme celle de Lotus/Notes - n'étant pas compatible avec la messagerie Internet standard - comporte une fonction de passerelle qui permet d'envoyer et recevoir des messages électroniques sur Internet (en plus de la messagerie Notes).

Path:

Liste les différents MTAs qui ont été traversés par le message. Cet en-tête est le plus souvent absent des en-têtes de courrier électronique parce qu'il est sensé ne concerner que les messages d'origine Usenet. Mais certains logiciels qui gèrent ces deux aspects (courrier électronique et forums de discussion) exploitent cet en-tête dans les deux cas.

PC-Pine

Logiciel de courrier électronique développé à l'Université de Washington et normalement utilisable sur MS-DOS, Microsoft Windows et Unix. Mais il a aussi été adapté à une multitude d'autres machines (allant de l'Amiga à VMS).

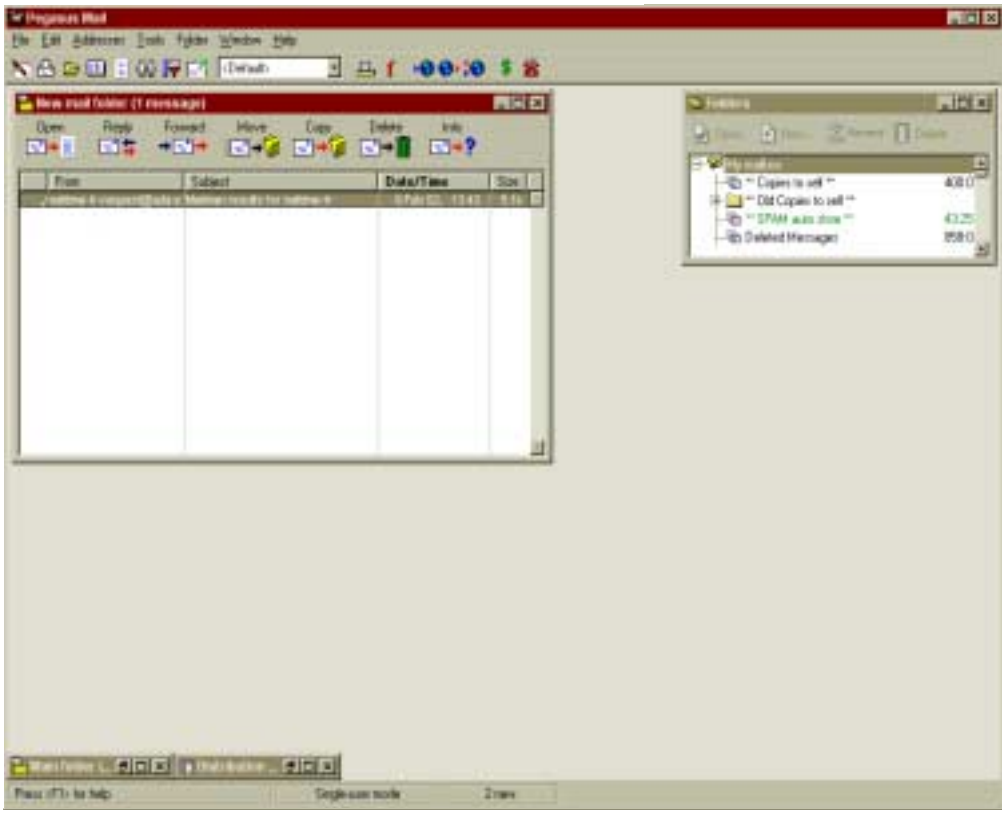
http://www.washington.edu/pine/

PeaceFire

Un site web qui s'active dans la lutte contre le SPAM et a gagné quelques procés contre des spammeurs.

http://www.peacefire.org/anti-spam/

Pegasus mail



Logiciel de courrier électronique gratuit produit par David Harris.

Pegasus mail est souvent considéré comme un outil un peu difficile d'abord parce qu'il comporte beaucoup d'options de configuration et favorise plutôt un type d'utilisateurs qui a déjà une certaine expérience du courrier électronique sur Internet.

Il est toutefois apprécié pour sa combinaison de caractéristiques qui en fait un outil appréciable pour les utilisateurs particulièrement exigeants ou ayant à gérer un nombre important de comptes de messagerie électronique.

Il existe des extensions gratuites qui permettent de lui faire parler français, allemand et quelques autres langues. Le logiciel et la documentation électronique sont gratuits. Néanmoins, la documentation et les manuels sont disponibles auprès de l'auteur sous une forme imprimée contre paiement.

http://www.pmail.com/

PEM

Privacy Enhanced Mail.

Un protocole d'échange de messages e-mail signés et/ou cryptés. N'a pas eu un grand succés.

PGP

Pretty Good Privacy.

Cet outil de base de la cryptographie informatique (l'art de rendre une information incompréhensible par les personnes qui n'ont pas de raison de la connaître) est connu pour être le premier outil de ce type facilement accessible alors que la technologie a longtemps été considérée comme l'apanage exclusif des

militaires et des espions. PGP est utilisé pour assurer l'inviolabilité des communications (et spécialement dans le cas de courriers électroniques).

Toutefois, il est important de noter que le terme « accessible » ne doit pas être confondu avec « simple d'emploi ». Même si PGP et les outils qui l'emploient peuvent être acquis par le commun des mortels, ils restent d'un usage compliqué (en particulier, quand on souhaite assurer une véritable confidentialité à ses communications).

Son caractère librement accessible (y compris les sources du logiciel) lui ont donné une importante visibilité médiatique et une certaine solidité reconnue dans l'exigente communauté des informaticiens qui se préoccupent de sécurité. Son créateur (Phil Zimmermann) a connu plusieurs fois la faveur des médias. Par exemple, il aurait probablement préferrer éviter l'arrestation par le FBI sous l'accusation de violation de la loi américaine sur l'exportation des moyens de cryptographie (qui sont classés parmi les armes de guerre aux USA et en France, comme dans de nombreux autres pays).

Par ailleurs, les préoccupations contradictoires de sécurité personnelle ou nationale et de protection de la vie privée mettent son usage au cœur de discussions acharnées de la part de partisans parfois très actifs.

http://www.pgp.org/

Phone:

Un en-tête non standard pouvant indiquer le numéro de téléphone de l'expéditeur.

Pièce jointe

Terminologie introduite par Microsoft pour les fichiers attachés. Voir « fichier attaché ».

Piège à SPAM

Afin de détecter les spammeurs, il existe une méthode relativement sure qui consiste à créer un piège à SPAM ou un « pot de miel ». C'est en général une adresse e-mail fictive qui n'est jamais utilisée que pour recevoir les courriers électroniques des spammeurs. Cette adresse est publiée à des endroits et sous des formes qui ne doivent pas justifier la réception d'un courrier électronique normal (par exemple, l'adresse peut apparaître en tout petits caractères en bas d'une page web qui ne propose aucun service et qui demande de ne pas écrire à cette adresse ; ou elle peut être employée dans la signature d'un post Usenet dans un groupe de discussion à faible trafic à la suite d'un message qui indique clairement qu'il s'agit d'un message destiné à piéger les spammeurs).

De nombreux opposants actifs au SPAM utilisent cette technique sous une forme ou une autre. Par exemple, je possède à tout moment deux adresses e-mail de ce type qui sont publiées temporairement ici ou là avec l'indication que je ne souhaite pas y recevoir de courrier électronique. Cela marche étonnament bien (les êtres humains comprennent que cela ne les concerne pas, mais les robots collecteurs d'adresses gobent l'hameçon jusuq'à la ligne). Cela confirme souvent facilement qu'un courrier électronique reçu sur une autre adresse valide fait bien partie d'un ensemble de gros volume.

ping

L'outil de base permettant de contrôler si un site ou une adresse est accessible.

Exemple d'exécution du programme ping sur Windows 98 (contrôle de la présence de la machine www.magic.fr) :

```
D:\USR>ping www.magic.fr

Envoi d'une requête 'ping' sur www.magic.fr [195.115.16.3] avec 32 octets de données :

Réponse de 195.115.16.3 : octets=32 temps=14 ms TTL=243
Réponse de 195.115.16.3 : octets=32 temps=21 ms TTL=243
Réponse de 195.115.16.3 : octets=32 temps=43 ms TTL=243
Réponse de 195.115.16.3 : octets=32 temps=21 ms TTL=243

Statistiques Ping pour 195.115.16.3:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en milli-secondes :
    minimum = 14ms, maximum =  43ms, moyenne =  24ms
```

L'utilisation de ping pour tester la présence d'une machine ou d'un serveur est considérée comme une pratique raisonnable et plus tolérable que de tester directement un port de communication. Le renseignement fourni par ping (la simple présence ou absence de la machine) est moins riche (on ne sait pas si le serveur est accessible pour le courrier électronique), mais dans de nombreuses situations le simple fait de tester un port sans y avoir été autorisé préalablement peut être interprété comme une tentative d'effraction (punissable par la loi).

On notera également, que l'absence de réponse de la part d'une machine n'est pas automatiquement synonyme de l'absence de cette machine. Certains logiciels de protocole IP (on parle souvent de « pile de protocole ») ne reconnaissent pas la demande ICMP de ping ; certaines machines sont configurées pour ne pas révéler leur présence même à un ping tout à fait innocent (c'est le cas depuis longtemps de www.ibm.com, par exemple[20]) ; certains routeurs et certains logiciels pare-feu ne laissent pas passer les paquets ICMP d'une commande ping afin de révéler le moins de choses possibles sur la structure interne d'un réseau protégé.

Voir aussi traceroute et Sam Spade.

Play By Mail (PBM)

Il s'agit d'une catégorie particulière de jeux électroniques qui reposent sur le principe du jeu par correspondance amélioré par l'emploi du courrier électronique (« jouer par e-mail »). On trouve un peu de tout dans cette famille, dont des jeux de rôle, des simulations économiques ou sportives, des jeux de pronostic ou de stratégie, etc. Le site « Les autres mondes » (http://www.lesautresmondes.net/) n'en recense pas moins de 400.

La passage du courrier papier au courrier électronique a - essentiellement - permis d'automatiser les fastidieuses opérations de dépouillement des « ordres » des joueurs. Cette libération a permis d'envisager des jeux dans lesquels les joueurs sont très nombreux et la durée des tours relativement courte (on n'est plus nécessairement restreint par les délais de la poste).

20 En réalité, il n'y a pas une machine www.ibm.com et donc la réponse à un ping serait probablement difficile à interpréter dans la quasi-totalité des cas.

Plus (« adresses à + »)

Certains routeurs de courrier électronique (comme les versions les plus récentes de sendmail) reconnaissent une forme inhabituelle d'adresse de courrier électronique où le nom de l'utilisateur peut être complété par un commentaire.

Par exemple :

utilisateur+commentaire_de_test@SpamAnti.net

Ici, l'adresse est équivalente à utilisateur@SpamAnti.net, mais cela permet d'ajouter le commentaire « commentaire_de_test ».

Notez bien que cette forme n'est que rarement reconnue pour le transfert de courrier d'un domaine à un autre.

Pollupostage

Autre nom (francophone celui-là) donné au SPAM.

Polluriel

Autre nom (francophone et probablement québecois) donné au SPAM.

Ponzi

Les « Ponzi schemes » (ou montage de Ponzi, en français) sont une classe à part d'escroqueries qui ont connus leur heure de gloire en 1920 lors de leur invention par Carlo “Charles” Ponzi. Il avait remarqué la possibilité de revendre aux USA des coupons de Poste internationale achetés en Espagne ou en Italie, en faisant un bénéfice considérable. Le seul problème est que les délais, les coûts annexes pour mettre en place une vraie organisation internationale pour en tirer parti coulaient complètement la fausse « bonne » idée. Alors, Ponzi a décidé de gagner de l'argent en vendant l'idée elle-même (il promettait un bénéfice de 50% en 45 jours). Complétement débordé par le succés, Ponzi vendait des titres dont le bénéfice n'était supporté que par les ventes de nouveaux titres. Ce qui devait arriver arriva : après avoir encaissé des millions de dollars (de l'époque !), la justice a demandé l'arrêt de l'encaissement de nouveaux clients et les anciens ont continué à demander les remboursements. 40 000 personnes se sont retrouvées emportées par la faillite qui a suivi et Ponzi a fait cinq ans de prison.

La législation américaine interdit explicitement ces montages financiers qui reposent sur du vent et ne peuvent tenir qu'un temps avant d'exploser littéralement sous le poids des engagements pris (et qui n'étaient tenus que grâce à l'arrivée de nouveaux clients/gogos).

POP3

Post Office Protocol version 3.

Protocole de communication utilisé pour collecter du courrier électronique stocké sur un serveur de messagerie.

L’avantage principal de ce protocole est de comporter une authentification de l’utilisateur (qui n’est pas présente dans SMTP). Cela permet de respecter une certaine confidentialité/sécurité pour l’accès aux boîtes-à-lettres des utilisateurs d’un serveur de messagerie.

Certains prestataires de courrier électronique fournissent un service de messagerie avec des boîtes-à-lettres accessibles par le protocole POP3. La plupart d'entre eux sont aussi (et avant tout) des

Fournisseurs d'Accès Internet qui incluent ce service dans leur prestation globale. Toutefois, vous serez peut-être intéressé d'apprendre que ce service est parfois indépendant de toute autre offre.

On ne rencontre que rarement ce genre de service à titre entièrement gratuit (il impose une contrainte forte sur l'espace disque qui doit être mis à disposition des clients).

Je ne peut pas vous signaler utilement de prestataires de ce type. Toutefois, le site anglophone http://www.internetemaillist.com/POP3/ présente utilement un certain nombre de ces services.

Pornographie

Et oui ! Le sexe reste bien un des meilleurs moyens de gagner de l'argent et la pornographie un des sujets les mieux représentés dans les messages de SPAM.

Port 25

Un numéro de port est le fruit d'un accord entre un serveur et un client établissant une communication de type IP. Le port 25 est particulier parce que c'est celui le plus souvent utilisé par les machines qui veulent communiquer en utilisant le protocole SMTP. Les personnes qui font de la mise au point de logiciels ou de protocoles de messageries de courrier électronique voient rapidement ce numéro de port devenir une référence incontournable.

Les assignations de port standard sont publiées par l'IANA sur son site web.

http://www.iana.org/assignments/port-numbers

Postfix

Une passerelle SMTP courante sur Unix, Linux, etc. créée par Wietse Venema, autorisant une gamme étendue de modifications des messages qui lui sont confiés et largement considérée comme une alternative intéressante à sendmail. Une attention particulière a été apportée à maintenir une certaine compatibilité avec sendmail afin de ménager ses utilisateurs qui voudraient passer à postfix.

Il a été précédemment connu sous d'autres noms : VMailer, puis IBM Secure Mailer (à partir de fin 1998).

http://www.postfix.org/

Postini

Un gestionnaire de serveur(s) de courrier électronique qui intègre de nombreuses fonctions de haut de gamme en plus de services anti-SPAM et anti-virus.

http://www.postini.com/

Postmaster

Le postmaster est un utilisateur très particulier du courrier électronique. Selon le RFC 2821, il existe nécessairement un « postmaster » pour tout domaine et tout site de courrier électronique.

Par exemple, pour le domaine SpamAnti.net, il s'agit d'un utilisateur (et d'une adresse électronique de la forme postmaster@SpamAnti.net) qui est capable de

Extrait du RFC 2821 (sur le protocole SMTP) :

4.5.1 Minimum Implementation

In order to make SMTP workable, the following minimum implementation is required for all receivers.

[...]

Any system that includes an SMTP server supporting mail relaying or delivery MUST support the reserved mailbox "postmaster" as a case-insensitive local name.

traiter les problèmes techniques liés à l'acheminement et à la gestion du courrier électronique dans ce domaine.

Il est également obligatoire qu'il s'agisse d'une personne véritable (et non pas un automate), en particulier parce que cette adresse est employée pour envoyer des messages d'erreurs complètement automatiques. Sinon, il y aurait le risque de voir deux automates s'échanger aveuglément (et indéfiniment) des messages d'erreurs.

Pourriel

Autre nom (francophone celui-là) donné au SPAM.

Precedence:

Certains logiciels de gestion de listes de messagerie (ou parfois certains logiciels de SPAM) indiquent explicitement que l'envoi est fait en masse. Supposément, cela permet à des serveurs d'agir sur la priorité de ces messages. Cet en-tête semble ne vraiment prendre que la valeur *bulk* (en masse) et ne pas exister sous une autre valeur.

Exemple :

Precedence: bulk

Prêtre, SPAM pour devenir

Parmi les SPAMs les plus curieux rencontrés au cours de mes années de collecte et de collection, on trouve cette série proposant d'ordonner des prêtres (plus exactement des ministres de culte) avec la promesse (assez américaine, il est vrai) de vous permettre de sceller des mariages, d'organiser des baptêmes et des funérailles, de donner très officiellement des conseils religieux ou de visiter des prisons ou des hôpitaux.

Le plus curieux était la promesse d'ordonner ces ministres en choisissant sa religion (catholique, protestant, juif ou autre). L'œcuménisme a parfois du bon (au moins pour assurer la rentabilité économique).

Prevent-NonDelivery-Report:

Un en-tête qui permet de refuser l'envoi du rapport de non-livraison d'un message (dans le cas où celui-ci n'est pas bien arrivé à son destinataire). RFC 1327.

Priority:

Cet en-tête permet de donner un niveau de priorité à un message. Il est plus ou moins bien géré, mais le principe veut que les correspondances suivantes soient utilisées :

Priority:	*Signification*
Priority: urgent	Priorité maximale (urgent)
Priority: normal	Priorité normale

Exemple :

Priority: urgent

On notera en particulier, que les informations de priorité sont rarement traitées pour les petits messages (il est plus simple de les expédier sans aucun traitement de priorité) et quand il n'y a aucun engorgement particulier (le cas le plus courant).

Devant les évidentes limitations de ce type de priorité à deux niveaux seulement, certains fournisseurs ont adopté un système plus complet, mais explicitement optionnel. Voir X-Priority: et X-MSMail-Priority:.

Prix d'une adresse

Tout a un prix ! Votre adresse de courrier électronique également. Par exemple, pour un spammeur, une base de données de 60 millions d'adresses se vend généralement aux alentours de 100-150$, si cette base de données comporte un nombre significatif d'adresses « vérifiées ». A défaut, le prix tombe plutôt aux alentours de 40-75$. Cela met quand même l'adresse de courrier électronique aux alentours de... ouh-la-la ! vraiment pas grand-chose.

Quoi qu'il en soit, on peut aisément remarquer que les adresses vérifiées coûtent deux à quatre fois plus cher que les adresses non triées (qui contiennent parfois plus de 50% d'adresses complètement erronées). C'est une excellente raison pour ne pas répondre aux spammeurs. En effet, dans le cas le pire, le spammeur apprend ainsi que votre adresse existe bel et bien et il peut la revendre à un de ses compères en faisant un (petit) bénéfice.

procmail

Un outil de traitement du courrier électronique. Il s'agit de manipuler les messages (par exemple, mais pas uniquement, pour assurer un filtrage). Cet outil permet à un utilisateur (généralement sur Unix ou Linux) de manipuler le courrier électronique reçu à condition de disposer de quelques connaissances de programmation.

http://www.procmail.org/

Pronto Mail

Un client de courrier électronique qui semble avoir de grandes qualités de simplicité au moins dans sa version « family edition ».

Protocole

Les communications informatiques impliquent que les ordinateurs intervenants soient précisément d'accord sur le contenu des informations à échanger et sur leur sens. Cet ensemble partagé de significations est appelé un protocole. Le courrier électronique utilise nombre d'entre eux dont les plus connus sont les protocoles SMTP et POP-3.

Pump and dump

On pourrait traduire par « gonflé puis abandonné » cette expression anglaise qui décrit une pratique relativement courante à la Bourse et qui a attiré des spammeurs. La méthode est simple : on contacte le plus de gens possible pour leur « apprendre » qu'une société côtée en Bourse va monter. Si on a acheté des titres auparavant, les gogos se précipitant tous ensemble pour suivre le « tuyau » miracle (« pump »), il suffit de vendre en faisant un bénéfice substantiel et de laisser retomber ensuite le soufflé (« dump »).

La plupart des gogos ne remarquent même pas que « l'information » qu'ils reçoivent est tout simplement un déli d'initié et qu'il est peu probable que quelqu'un en fasse profiter des millions de gens sur Internet. Ils se laissent appater. Et quand l'escroc a fait fructifier son pactole, ils se retrouvent avec des titres qui ne valent rien (ou si peu par rapport à ce qu'ils ont payé).

Afin que les choses soient bien claires dans ce domaine, je me permets d'insister sur le fait que cette pratique (comme beaucoup d'autres escroqueries petites ou grandes à la Bourse) est totalement illégale dans la quasi-totalité des pays du monde. Les marchés sont surveillés spécifiquement pour cela, des enquêtes sont diligentées à la moindre plainte et des sanctions sévères sont prises à chaque fois que le coupable peut être identifié. Mieux, étant donné les sommes mises en jeu dans la plupart des cas, les « gendarmes de la Bourse » sont souvent beaucoup plus actifs dans cette répression que la police ou la gendarmerie pour ce qui concerne les autres escroqueries utilisant des hautes technologies[21].

Voir l'article « Bourse ».

3.18. Q

qmail

Un Mail Transfer Agent développé par D.J. Bernstein et qui se rencontre sur Unix et GNU/Linux (il est compatible avec sendmail) et est souvent utilisé pour gérer des listes de messagerie. Ses partisans vantent ses qualités en termes de sécurité (depuis mars 1997, il y a un prix de 500$ pour la première personne à publier une faille de sécurité dans ce produit ; personne ne l'a gagné ; personne n'a trouvé une telle faille).

Certainement, un des plus couramment utilisés après sendmail (d'après le SMTP Gateway Survey présenté à http://www.bbv.com/SMTP-Survey.htm).

http://cr.yp.to/qmail.html

3.19. R

RBL

Realtime Black List.

Un type de liste noire organisée en temps réel par certains fournisseurs d'accès pour permettre de « prendre de vitesse » les spammeurs les plus ennuyeux. La plupart de ces « listes noires » gèrent les inscriptions et retraits de machines identifiées comme des « open relays ». La gestion automatique est rendue nécessaire par le caractère Temps Réel de ces services qui répondent avec un très faible aux requêtes d'information et qui sont mise à jour de seconde en seconde en fonction des plaintes et des tests effectués.

Quelques RBL significatives :

Nom	*Site web*	*Remarques*
ORBS		A cessé toute activité en 2001, sous la pression d'un spammeur.
ORBL	http://www.orbl.org/	

21 Dans un certain nombre de cas, la maraichaussée, un peu débordée par la technicité des enquêtes, « laisse tomber » là où la Securities and Exchange Commission (la SEC aux USA) ou la Commission des Opérations de Bourse (la COB en France) ou le BaFin (en Allemagne) engagent des poursuites très précises et véritablement décidées à aboutir.

Nom	*Site web*	*Remarques*
ORBZ	http://www.gst-group.co.uk/orbs	A cessé toute activité en 2002, face à une action en justice qui n'était que partiellement liée à son contenu.
ORDB	http://www.ordb.org/	
Vix	http://www.vix.com/rbl/	Sans doute le premier. A cessé son activité

Received:

Un des en-têtes les plus difficiles à décoder dans un courrier électronique. Sa forme est parfois très approximative, variable d'un message à l'autre, etc. En fait, chaque serveur ou MTA par lequel passe un message électronique est sensé ajouter un ou plusieurs en-têtes de type Received: afin de documenter le trajet suivi.

Il est rare (mais pas impossible) de rencontrer des MTA qui retirent les en-têtes Received: quand ils estiment qu'il y en a trop. Il est habituel qu'un SPAM contienne un ou plusieurs en-têtes Received: purement et simplement inventés pour perdre celui ou celle qui cherche à trouver l'origine d'un SPAM.

Un exemple de séquence complète d'en-têtes Received: apparaît ici :

```
Received: (qmail 50424116 invoked by uid 0); 9 May 2002 11:39:27 -0000
Received: from unknown (HELO redir.gandi.net) ([80.67.173.6]) (envelope-sender <yr@SpamAnti.net>)
        by 212.198.2.75 (qmail-ldap-1.03) with SMTP
        for <Roumazeilles@noos.fr>; 9 May 2002 11:39:27 -0000
Received: from uponart.com (e047.dhcp212-198-23.noos.fr [212.198.23.47])
                by redir.gandi.net (Postfix) with ESMTP id E36DF30015
                for <Yves@Roumazeilles.net>; Thu,  9 May 2002 13:39:26 +0200 (CEST)
Received: from Spooler by uponart.com (Mercury/32 v3.30) ID MO001545;
   9 May 02 13:38:08 +0200
Received: from spooler by uponart.com (Mercury/32 v3.30); 9 May 02 13:36:12 +0200
Received: from champagne (192.168.0.15) by Champagne (Mercury/32 v3.30) with ESMTP ID MG001543;
  9 May 02 13:34:25 +0200
```

On remarque aisément dans un tel exemple (sans aucune tentative de fraude ou de dissimulation) que le « décodage » et la compréhension de ce genre de séquence demande un entrainement qui n'est pas forcément immédiatement accessible à tous les utilisateurs.

De plus, on remarquera rapidement que la forme des ces en-têtes est très variable et ne répond pas nécessairement à un standard commun.

Redirection

Voir aussi « bounce ».

References:

En-tête rare en dehors du contexte de courrier électroniques utilisés en parallèle des envois (*posts*) sur les groupes de discussion Usenet. Il permet de retrouver l'envoi (le *post*) qui se trouve plus haut dans la hiérarchie des envois (*posts*), généralement le message auquel on répond. Dans le courrier

électronique, cet en-tête indique un ou plusieurs autres messages liés logiquement au message qui le contient.

Relais ou relay

Le transfert d'un courrier électronique se fait rarement directement de la machine de l'expéditeur à la machine du destinataire. Au contraire, ces machines passent souvent par l'intermédiaire d'ordinateurs relais. Ils reçoivent le courrier électronique qui leur est destiné (et qui va être stocké localement) mais aussi du courrier qui ne leur est pas adressé (qu'ils vont renvoyer vers sa destination). Ces machines intermédiaires sont appelées « relais ».

Un relais est donc une machine qui fait une partie du travail de l'envoi de courrier électronique. Aux débuts du courrier électronique et d'Internet, la plupart des ordinateurs capables de traiter du courrier électronique acceptent de jouer le rôle de relais pour qui le demandait. Cela le soumet au risque de se voir « utilisé » par quelqu'un qui n'y est pas autorisé. Alors que c'est pratique pour corriger discrètement les erreurs de routage (il y aura toujours une machine pour remettre votre courrier « sur les rails »), et que c'est à peu près sans conséquence quand il s'agit de relayer un ou deux courriers électroniques, cela peut devenir dramatique si l'indélicat a l'intention d'envoyer 15 millions de courriers électroniques d'un seul coup[22].

Dans le cas d'un relais qui ne fait aucune distinction dans les courriers qu'il reçoit (et qu'il achemine gentiment), on parle de « open relay » (ou relais ouvert, en bon français). Les machines ainsi configurées sont aujourd'hui chassées et poursuivies avec acharnement par les partisans de la lutte contre le SPAM parce que leur « mauvaise » configuration crée pour les spammeurs une opportunité d'envoyer littéralement des millions de courriers électroniques depuis un petit PC en quelques minutes seulement (tout le « travail » étant fait par la machine relais, qui peut éventuellement se retrouver occupée par cette seule tâche pendant plusieurs jours d'affilée).

On remarquera qu'un serveur de messagerie qui est configuré en open relay est une cible potentielle pour les robots qui sont utilisés quotidiennement par les spammeurs afin de trouver ce type de victime à exploiter. Il est vivement conseillé de ne pas attendre l'agression qui ne peut manquer de venir pour fermer cette notable faille de sécurité. La réparation au cours d'une séance d'exploitation par un spammeur est particulièrement difficile même pour un administrateur réseau expériementé, alors qu'il s'agit d'une opération relativement simple avant le début de l'agression.

De manière très pratique (mais en anglais), le site de Mail Abuse Prevention System (MAPS) propose des conseils précis pour permettre à un administrateur de réseau de modifier la configuration de son logiciel serveur de messagerie afin d'interdire un éventuel « open relay » :

http://mail-abuse.org/tsi/ar-fix.html

En 2001, la société IMC a essayé d'évaluer le nombre « d'open relay » existant. En vérifiant les serveurs SMTP en janvier 2001, ils ont trouvé 6% de machines configurées de cette manière. Cela reste un chiffre considérable mais en baisse notable par rapport aux 17% observés un an et demi auparavant, démontrant l'amélioration d'une situation qui reste d'autant plus préoccupante que les serveurs étudiés étaient seulement des serveurs de domaines officiels et que cela ne comptait pas les machines qui ont seulement une adresse IP, mais pas de nom de domaine associé (la majorité des internautes connectés à haute vitesse, par exemple).

22 Malgré les apparences, ce chiffre n'a rien d'anormal ou d'énorme. J'ai reçu la proposition d'un CD-ROM avec 60 millions d'adresses (dont une garantie de validité) pour seulement 40$, y compris « le logiciel qui permet d'envoyer 30 000 SPAMs par heure ».

Relay rape

En français « viol de relais ». Voir ce terme.

Remailer anonyme

Service qui permet de rendre anonyme un courrier électronique en le ré-expédiant après avoir effacé les informations présentes dans les en-têtes et qui permettraient l'identification de l'origine du courrier électronique.

De fait, le simple terme « remailer » est souvent utilisé pour décrire un « remailer anonyme ».

Voir aussi anonymizer.

Remove

En français *retrait* ou désabonnement. Dans de nombreux messages de SPAM, on trouve une proposition de retrait de la liste de messagerie qui a servi à l'envoi du SPAM. Ce service de retrait (souvent intitulé en anglais *Remove* ou *Remove-me*) est généralement un leurre. Je vous conseille de ne pas l'employer.

- La plupart des spammeurs n'utilise qu'une seule fois la liste qu'ils ont achetée.
- Dans le cas d'un SPAM traditionnel, le service de retrait n'existe souvent tout simplement pas. Ou il s'agit d'une *drop box*.
- Dans le cas d'un SPAM traditionnel, le service de retrait ne sert qu'à confirmer au spammeurs que votre adresse est valide (après cela, votre adresse pourra être revendue plus cher qu'auparavant, mais cela ne risque pas de réduire le SPAM reçu).

Les cas où il est utile et souhaitable d'employer les Remove-me :

- Quand vous vous êtes vous même inscrit sur la liste. Dans ce cas, on peut supposer une certaine bonne volonté de la part de votre correspondant.
- Dans le cas d'une liste de retrait organisée par une entreprise, une association ou un organisme dans lequel vous avez confiance. Leur efficacité repose essentiellement sur la volonté des spammeurs d'utiliser ces services (tout semble indiquer qu'il n'en est absolument pas le cas). Mais cela ne risque guère de faire de mal.

Les conseils donnés ici ne sont pas des absolus mais ils proviennent de mon expérience. Dans tous les cas, malgré les apparences, il est moins « risqué » de ne rien faire que de tenter de se désinscrire.

Reply-to:

Cet en-tête indique une adresse à laquelle renvoyer préférentiellement une réponse. Il doit normalement être utilisé quand on appuye sur le bouton « Répondre » d'un logiciel de messagerie (au lieu de répondre à l'adresse qui était indiquée dans l'en-tête To:).

Répondre ou reply

Dans le contexte d'un logiciel de courrier électronique, action qui consiste à répondre à un message par un autre message. Il est habituel (et considéré comme poli) de citer une partie au moins du message original.

Exemple :

> pouvons-nous nous rencontrer demain à midi ?
> Pierre
Pas de problème, je serai-là avec Jean.
Henri

Réponse automatique

Certains logiciels et certains serveurs de courrier électronique comportent une fonction de réponse automatique. Cela permet d'assurer certains services appréciables comme de prévenir vos correspondants de votre absence.

On remarquera qu'il convient d'être très attentif à l'usage que l'on fait d'une telle fonctionnalité si l'on veut éviter le risque significatif de voir deux programmes de réponse échanger des messages automatiques pendant des journées entières et saturer totalement des serveurs et des boîtes-à-lettres (des programmes complètement automatiques risquent de ne pas se fatiguer d'envoyer des dizaines de milliers de message, là où un utilisateur humain remarquerait très vite un problème).

On notera que c'est une raison pour laquelle le RFC 2821 impose que l'adresse postmaster ne soit jamais équipée d'un programme de réponse automatique : deux postmasters pourraient facilement se retrouver en train d'échanger des messages d'erreur à une vitesse plus élevée que la capacité de l'administrateur à les arrêter.

Réputation

Au delà du fait très général que la réputation d'une entreprise (ou d'une personne) se joue dans la qualité des messages de courrier électronique qu'elle distribue (comme les courriers « papier » qu'elle poste), il faut remarquer que le SPAM ternit rapidement la réputation des sociétés qui ont quelque imarge de marque à défendre.

Certains en ont fait les frais ces dernières années et la plupart des grandes entreprises ont appris à établir des règles très strictes dans ce domaine. Beaucoup de PME/PMI n'ont pas encore compris ce message et pratiquent (ou tentent de pratiquer) le SPAM sans se rendre compte des dégats considérables que cela peut causer sur le moyen et le long terme. Par exemple, les messages échangés entre les combattants anti-SPAM sont souvent enregistrés dans des archives de listes de messagerie ou de groupes de discussion pour des années au moins. Ainsi, il est relativement aisé de retrouver tous les cas de SPAM d'une société remontant à 1997. Cette tâche restera pendant encore longtemps sur le nom de certaines entreprises - même après avoir cessé complètement d'utiliser le SPAM.

A l'opposé, il arrive (très rarement, mais de manière observable tout de même) que quelqu'un de mal intentionné se fasse passer pour une entreprise ou un de ses employés pour envoyer un SPAM au plus grand nombre de personnes. Ce genre de situation ne doit pas être pris à la légère par les entreprises ou les organisations qui en sont victimes. Autant une action rapide et déterminée peut limiter les dégats et permettre de retrouver la trace du coupable, autant l'inaction se traduit par des conséquences de plus en plus ingérables.

Resent-Date:

Cet en-tête est utilisé par les programmes qui servent à tester une liaison de courrier électronique. Généralement, le contenu de Date: y est recopié, si une date plus précise ne peut pas être fournie.

Voir également l'article « loopback » pour plus de détails sur ces outils de test.

Responsabilité sociale

Les différents acteurs d'Internet et les différents utilisateurs du courrier électronique partagent une réelle responsabilité sociale dans la mesure où Internet est un media qui s'appuie fortement sur une large distribution/diffusion des charges et des responsabilités.

Utilisateurs

A ce titre, les utilisateurs sont directement impliqués par l'usage qu'ils font de leur courrier électronique (et des autres outils Internet, bien sûr). Pour ne citer qu'un exemple, chacun doit se sentir socialement obligé à ne pas diffuser les rumeurs et autres canulars. Plus encore, lorsqu'il en reçoit, l'utilisateur a la responsabilité de les arrêter, de trouver et de diffuser les informations exactes qui permettent de les contrer.

Chacun se doit de penser à limiter l'impact de ses actions en faisant simultanément preuve de réserve, de retenue et de politesse. C'est à ce prix que les listes de discussion restent une source exploitable d'information, par exemple.

Chacun se doit d'avoir un logiciel anti-virus tenu à jour afin d'éviter d'être propagateur de virus, vers et autres infections qui sont préjudiciables à tous lorsqu'elles prennent de l'ampleur.

Administrateurs de réseau

La charge de maintenir son réseau (et en particulier les serveurs de courrier électronique) est centrale dans ce métier et cette activité. Mais, il faut garder à l'esprit qu'il ne s'agit pas seulement de viser l'efficacité optimale dans un contexte minimal. Deux exemples sont flagrants : dans certains cas, laisser un serveur de courrier électronique en configuration « open relay » sera sans importance très significative (bande passante importante, serveur normalement surdimenssionné, par exemple) ; et pourtant refermer cette porte ouverte aux spammeurs est une responsabilité envers tous les autres utilisateurs de courrier électronique dans le monde. Par ailleurs, l'administrateur réseau a une obligation morale considérable de se tenir au courant des sujets concernant la sécurité des systèmes dont il a la charge. Trop de systèmes sont propagateurs de virus ou de vers par pur laxisme.

Fournisseurs d'Accés Internet (FAI)

Les Fournisseurs d'Accés Internet, comme représentants de groupes importants d'internautes et comme exploitants de systèmes plus considérables que la moyenne, ont des responsabilités similaires à celles de leurs utilisateurs et de leurs administrateurs, mais s'y ajoutent aussi celle de former leurs clients, celle de les représenter dans les instances techniques et celle de promouvoir des solutions qui vont dans le sens de l'amélioration non seulement de leur propre service mais aussi du fonctionnement général du réseau. Les actions autour du SPAM sont donc (ou devraient être) une priorité quotidienne pour les FAI.

Entreprises commerciales

Souvent tentées par la facilité de certaines pratiques électroniques (au premier rang desquelles se trouve le SPAM), les entreprises se doivent de participer activement à la mise en place des garde-fous et des moyens qui permettront de renforcer un moyen de communication dont le développement apportera à tous. Pensons à ce que serait aujourd'hui notre société si les entreprises avaient abusé à leur création du téléphone et du fax comme le font certaines avec le courrier électronique. Dans un espace où le législateur et le juge ne sont pas toujours surs des attitudes à adopter et font parfois un peu d'attentisme, les entreprises ont aussi la responsabilité de ne pas sur-exploiter Internet et de ne pas abuser de ses ressources. Il en va de l'intérêt de tous (entreprises comprises) à moyen terme.

Return-Path:

Un en-tête qui indique un chemin de retour (pour les messages d'erreur). Son remplissage est diversement effectué (ou modifié) par les MTA par lesquels transitent les messages de courrier électronique. Son contenu est donc malheureusement assez peu fiable.

Return-receipt-to:

Cet en-tête optionnel est habituellement utilisé par les logiciels de messagerie qui souhaitent recevoir un « accusé de réception » du courrier envoyé. Cette fonctionnalité très diversement supportée par les logiciels existants (certains n'en disposent pas du tout, certains ne l'autorisent que sous condition d'approbation par l'utilisateur, etc.) peut être la source de beaucoup de déception ou de surprises.

Voir aussi X-Confirm-Reading-To: et X-Rcpt-To:

RFC

Les RFC (ou Request For Comment) sont les documents de base qui organisent le fonctionnement d'Internet. Ils sont proposés par des individus ou des entreprises, débattus, amendés puis adoptés par l'Internet Engineering Task Force (IETF). Dans ce processus, il est important de distinguer les RFC qui sont devenus des standard de ceux qui sont restés des propositions ou des informations (on trouve en particulier une série de canulars lancés dans les RFC à l'occasion du 1er avril, comme cette méthode de transmission des paquets IP par l'intermédiaire de pigeons voyageurs[23]).

RFC	*Titre*	*Remarques*
821	Simple Mail Transfer Protocol	Complété et remplacé par le RFC 2821.
822	Standard for ARPA Internet Text Messages	Le RFC de base pour la syntaxe de la messagerie électronique (et des en-têtes). Complété et remplacé par le RFC 2822.
934	Message Encapsulation	
1327	Mapping between X.400(1988) / ISO 10021 and RFC 822	Ce RFC définit un certain nombre de nouveaux en-têtes qui sont utilisés dans les passerelles entre X.400 et le courrier Internet. Ces en-têtes sont donc relativement rares aujourd'hui (2002) et leur absence n'est pas préjudiciable. Ils sont toutefois susceptibles d'être plus présents dans le futur.
2045/2046/2047/2048/2049	Multipurpose Internet Mail Extensions	(MIME)

23 Pour ceux que cela peut intéresser, la méthode a été testée en 2001 par une université scandinave qui a appliqué à la lettre le RFC. Comme quoi certains canulars peuvent avoir la vie dure dans les milieux technophiles d'Internet.

RFC	*Titre*	*Remarques*
2076	Common Internet Message Headers	Les en-têtes de message électronique les plus courants.

Quelques-uns des Requests For Comment (RFC)
les plus courants pour la gestion du courrier électronique

RNIS

Réseau Numérique à Intégration de Services.

Traduction française du terme anglais ISDN, une des premières technologies numériques mises largement à la disposition du public pour apporter un réseau numérique à des clients connectés par téléphone (et donc jusque-là uniquement par modem traditionnel).

Cette technologie a eu un certain succès en Allemagne, un succès plus réduit aux Etats-Unis mais n'a jamais vraiment pénétré le marché français. Elle est actuellement totalement supplantée par les techniques haut débit comme le cable ou l'ADSL qui présentent simultanément un prix similaire (ou moindre) et une performance sensiblement plus élevée que les 128kb/s du RNIS à deux canaux.

Robot

On parle de robot pour les logiciels qui sont chargés de circuler sur une partie d'Internet (sur les sites web, ou dans les forums Usenet, par exemple) à la recherche d'une information.

On rencontre un nombre important de robots au service des spammeurs. Ceux-ci recherchent les adresses valides des internautes pour alimenter les bases d'adresses qui seront ensuite soit revendues à bas prix, soit utilisées directement pour produire du SPAM.

Nom du robot	*Id HTTP du robot*
ExtractorPro/WebWeasel	"Crescent Internet ToolPak HTTP OLE Control v.1.0" ou "ExtractorPro"
Harvester	"Crescent Internet ToolPak HTTP OLE Control v.1.0"
Web Mole	"Crescent Internet ToolPak HTTP OLE Control v.1.0"
Bull's Eye Gold	"Mozilla/2.0 (compatible; NEWT ActiveX; Win32)"
Maverick II	"Mozilla/2.0 (compatible; NEWT ActiveX; Win32)"
WebCollector	"Mozilla/2.0 (compatible; NEWT ActiveX; Win32)"
Cherry Picker	"CherryPicker/1.0" ou "CherryPickerSE/1.0" ou "CherryPickerElite/1.0"
Dynamic Web Wizard	"Microsoft URL Control - 5.01.4511"
Email Digger Pro	"Microsoft URL Control - 6.00.8140"
Email Collector	"EmailCollector/1.0"
Email Wolf	"EmailWolf 1.00"
NICErsPRO	"NICErsPRO"
Advanced Email Extractor	"Mozilla/4.0 (compatible; Advanced Email Extractor v1.3)" or ou toute autre chaine définie par l'utilisateur
Nitro	"Mozilla/3.Mozilla/2.01 (Win95; I)"
Sonic Email Collector	"EmailSiphon"

Nom du robot	*Id HTTP du robot*
Telesoft (by softcell.net)	"Telesoft/1.29"
WebBandit	"WebBandit/2.1" ou "WebBandit/3.50" ou "webbandit/4.00.0"
WebmailExtractor	"WebEMailExtractor/1.0B"
Zeus Internet Marketing Robot	"Zeus 2500 Webster Pro V2.9 Win32" (le chiffre 2500 peut varier)
List Sorcerer	"Mozilla/4.0 + (compatible; + MSIE + 4.01; + Windows + 95)"
Webmole 2000	"Mozilla/4.0 (compatible; MSIE 4.0; Windows NT)"
WebSnake	"Mozilla/3.0 (Win95; I)"

Quelques signatures de robots collecteurs d'adresses

NOTE : tous ces programmes ne sont pas utilisés exclusivement pour la production de SPAM, mais au moins pour la collecte d'adresses e-mail (et sont donc facilement détournés de leur usage original).

De nombreux autres programmes ne s'identifient pas ou fournissent une identité qu'ils usurpent à un navigateur du commerce (une quelconque version de Netscape Navigator ou d'Internet Explorer en général), comme certains de ceux qui sont identifiés ci-dessus. Cela impose la plus grande attention si vous souhaitez utiliser une telle liste pour « filtrer » les accès à votre site web (vous ne voulez sans doute pas qu'une fausse manipulation ou l'inscription d'une règle d'exclusion un peu trop aggressive ne vous conduise à refuser des visiteurs normaux).

Une excellente référence pour ces informations :

http://www.sendfakemail.com/fakemail/antispam.html

Roi du SPAM

Deux spammeurs particulièrement remarqués se sont autoproclamés « roi du SPAM » :

- Jeff Slaton en 1995 (de nombreux SPAM à caractère souvent sexuel provenant du Nouveau Mexique),
- Sanford Wallace, le propriétaire de Cyber Promotions, Inc.

RTFM

Selon les sources (plus ou moins argotiques), on traduit cette abréviation par « Read The Fine Manual » ou « Read The Fucking Manual ». C'est la réponse traditionnelle (et souvent sur un mode d'énervement) faite à une question dont la réponse est dans le manuel du produit dont il est question : « allez donc lire le manuel avant de poser une question stupide ».

C'est aussi (et surtout dans le contexte de l'encyclopédie du courrier électronique) le nom d'un serveur de fichiers qui est installé au Massachussets Institute of Technology (MIT) et accessible depuis des années par courrier électronique. L'adresse est mail-server@rtfm.mit.edu à laquelle on peut envoyer des commandes par email (et recevoir des réponses par email).

Typiquement, on rédige un courrier électronique avec un Subject: vide, et une commande dans le corps de texte. Une commande typique serait :

```
send usenet/news.answers/mail/country-codes
```

ou :

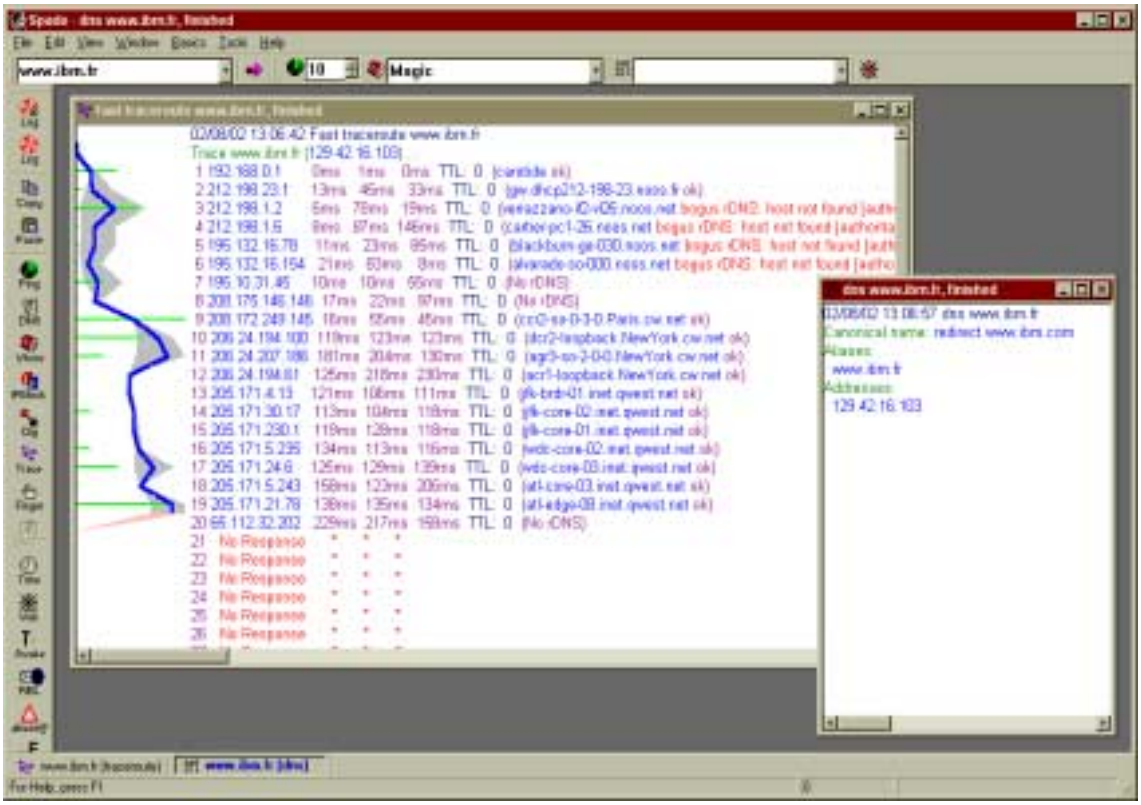
help

La première commande permet de se faire adresser une copie d'un document (en fait, une FAQ Usenet) ; la seconde permet de demander le fichier d'aide (en anglais) qui donne la liste des commandes du serveur de messagerie.

Ce serveur est une source permanente d'informations de base (parfois un peu datées, mais souvent techniquement ou culturellement très utiles).

3.20. S

Sam Spade



Site web et logiciel freeware pour Windows qui regroupent un ensemble très complet d'outils d'analyse réseau. Le logiciel pour Windows est considéré comme le couteau suisse du gestionnaire de réseau qui travaille depuis Windows.

Voir aussi ping et traceroute.

Le site web de Blighty Design : http://www.samspade.org/

Scam

Mot anglais qui désigne les escroqueries (ou tentatives d'escroquerie). On retrouve un nombre considérable de ces « scams » dans le courrier électronique (souvent sous la forme de SPAM puisqu'il y est important de pouvoir contacter un maximum de victimes dans un minimum de temps).

Secret

Le secret des communications électroniques (et donc par courrier électronique) est rarement garanti. Il est important de s'en préoccuper avant d'utiliser ces moyens pour transmettre des informations à caractère secret. En particulier, il est utile de s'appuyer sur les conseils de spécialistes tant les pièges sont nombreux dans le domaine de la gestion du secret électronique et des techniques d'encodage et de cryptographie.

Secret professionnel

La facilité avec laquelle un message peu être envoyé par courrier électronique peut faire oublier les règles élémentaires liées à la confidentialité de certaines informations et au respect du secret professionnel. Comme les accidents sont facilement arrivés, comme la dissimulation reste très difficile dans ce domaine, comme les entreprises sont souvent très sensibles aux conséquences de ce genre « d'erreurs », il est vivement conseillé de ne jamais oublier les règles de base concernant la confidentialité dans un contrat de travail ou un contrat entre entreprises.

See-Also:

Référence à d'autres articles Usenet liés logiquement à ce message.

sendmail

Le plus connu et un des plus anciens logiciel de messagerie. Fonctionnant généralement sur Unix, ce logiciel est souvent considéré - à juste titre - comme l'un des outils de messagerie les plus difficiles à maîtriser à cause d'une syntaxe inhabituellement complexe et peu tolérante (même dans le contexte des applications Unix de bas niveau qui ont déjà eux-mêmes une réputation de ne pas favoriser une interface utilisateur transparente). Toutefois, il a l'énorme avantage de permettre de créer des MTA extrêmement puissants et souples (par exemple, sendmail est prévu comme capable de modifier le contenu d'un message en fonction de règles de ré-écriture plus ou moins riches qui ne se limitent pas aux en-têtes).

L'ouvrage de référence :

sendmail, 2nd Edition

De Bryan Costales, avec Eric Allman

2e édition Janvier 1997

Editions O'Reilly

1-56592-222-0, 1046 pages

sendmail s'est longtemps constitué une réputation détestable dans les milieux de la lutte contre le SPAM en restant (trop) longtemps configuré par défaut comme un open relay. A cause de cela, tous les installateurs pressés ou peu au fait du problème laissaient leur serveur ouvert à tous les vents. Cela a heureusement changé aujourd'hui (depuis la version 5). Ce simple changement avait fait considérablement baisser le nombre de machines configurées en open relay dans le monde.

Exploiter une RBL depuis sendmail est aujourd'hui très facile puisqu'il s'agit simplement d'ajouter une ligne de commande dans le fichier de configuration .mc : pour les versions les plus récentes de sendmail, FEATURE(rbl,`spammers.v6net.org') ; pour les versions légèrement plus anciennes (mais v8.10 ou postérieures), FEATURE(dnsbl,`spammers.v6net.org') .

http://www.sendmail.org/

Sender:

La personne ou l'agent qui soumet le message au réseau dans le cas où ce n'est pas la même entité qui est citée dans l'en-tête From:.

Serveur de messagerie

Pour fonctionner, le courrier électronique repose sur l'existence d'ordinateurs spécialisés qui recueillent le courrier, le distribuent et le tiennent à la disposition des utilisateurs de logiciels de messagerie ou de courrier électronique. Ces machines communiquent par l'intermédiaire de protocoles particuliers (SMTP, POP3, etc.).

Sexe

Et oui Avec l'argent, l'un des plus puissants moteurs de l'humanité reste au cœur de beaucoup de SPAM et parfois de pures escroquerie à la santé.

Shareware

Logiciel distribué à bas coût et que l'utilisateur est invité à télécharger et à essayer. Si l'utilisateur l'apprécie suffisamment pour continuer à l'utiliser après un certain temps, il est plus ou moins vivement invité à l'acheter.

L'intérêt de cette méthode de diffusion est de favoriser le bouche-à-oreille positif (si vous appréciez le logiciel, vous êtes invité à en confier une copie à quelqu'un d'autre susceptible de l'apprécier également). Par ailleurs, les coûts de distribution sont bien moindres que pour un éditeur qui souhaite passer par les circuits de commercialisation traditionnels.

Ne pas confondre avec le freeware. Le shareware est bel et bien payant (contrairement au freeware). Mais il est possible de le tester avant de l'acheter.

Signature

Il est courant de finir un courrier électronique par un petit bloc de texte qui fait office de signature préformattée. La longueur de cette signature peut varier considérablement d'un utilisateur à un autre (d'une ligne à plusieurs dizaines). Mais il est considéré de bon goût de se limiter à quelques lignes seulement.

C'est un des rares endroits où il est considéré comme normal de faire de la publicité pour soit ou son entreprise sans que cela soit condamnable comme du SPAM, même s'il est souhaitable de se limiter à quelques mots ou une phrase pour décrire l'entreprise ou son produit-phare.

La signature doit normalement commencer par deux tirets, un blanc (ou un espace) et un retour à la ligne. Cette forme très précisement codifiée permet à certains logiciels de reconnaître ce qui fait partie du corps du message et ce qui n'en fait pas (par exemple, un gestionnaire de liste de messagerie reconnaîtra qu'il n'y a plus de commandes qui lui sont destinées à l'apparition du marqueur de signature et cessera d'interpréter le contenu du message).

Par exemple, ma signature de courrier électronique est le plus souvent :

```
--
Yves ROUMAZEILLES maintains SPAM.Anti! database and web site
27-31 rue Robert de Flers    Tél: +33 (0)1.45.75.92.75
75015 PARIS    (FRANCE)      GSM: +33 (0)608.750.486
mailto:info@SpamAnti.net     Fax: +33 (0)1.40.21.12.43
http://www.SpamAnti.net/
```

On remarquera qu'elle contient aussi bien des informations pratiques pour me joindre qu'un court message de publicité pour le site SPAM.Anti! et les adresses du site et de plusieurs de ses miroirs.

Signature électronique

La plupart des grands pays du monde sont en train d'adapter leur législation pour permettre l'emploi d'une signature électronique avec la même valeur de preuve qu'un paraphe en bas de page.

Pour l'Europe, une directive européenne du 30 novembre 1999 définit le cadre dans lequel doivent s'inscrire les lois nationales. L'Italie et l'Allemagne ont déjà modifié leur législation. La France, l'Espagne, le Luxembourg, le Royaume-Uni, la Belgique et le Danemark sont en passe de le faire.

Signature numérique

Une méthode de cryptographie pour prouver que le propriétaire d'une clé publique est bien l'auteur du message signé.

S/MIME

Secure MIME.

Standard qui comporte des options de sécurisation du courrier électronique comme l'encryptage (en vue d'interdire la lecture du contenu par un tiers) ou la signature (en vue de prouver l'origine d'un message ou de détecter la modification du message par un tiers).

Smiley

On traduit parfois ce nom anglais par *émoticon* ou *souriard* (expressions qui ne semblent guère avoir « pris » dans la langue française). Il s'agit de petits groupes de caractères qui, quand on les regarde en penchant la tête à gauche, semblent représenter un petit visage avec une expression plus ou moins bien définie par les caractères employés.

Ces smileys sont généralement employés pour faciliter la transmission d'une information qui ne passe pas très facilement dans un texte court (une émotion, un état d'esprit, un type de réaction). Certains utilisateurs en usent et en abusent. Parfois, on peut même rencontrer une forme de véritable recherche artistique dans leur construction.

Quelques exemples :

:-)	Sourire, satisfaction. Usage très courant.
;-)	Plaisanterie, clin d'œil. Usage très courant. Signifie que le texte est à prendre au second degré.
:-(	Tristesse, déception ou mécontentement. Usage courant.
:-/	Scepticisme.
:-D	Franche rigolade.
:-O	Cri ou surprise.

Il semble aujourd'hui démontré que l'inventeur des smileys est Scott Fahlman qui, le premier, en a fait la proposition sur le BBS « Computer Science general » de l'université de Carnegie-Mellon (CMU). Les gens qui y échangeaient des messages cherchaient un moyen de suggérer l'amusement ou la blague pure et simple. Dans un message du 19 septembre 1982, il propose « :-) » qui ne sera accepté que

lentement, mais va connaître un succés finalement planétaire. Le message lui-même a pu être retrouvé et peut être relu à l'adresse suivante :

http://www-2.cs.cmu.edu/~sef/Orig-Smiley.htm

SMS

Short Message Service.

La téléphonie GSM comprend un moyen de transmettre de courts messages textuels (jusqu'à 160 caractères). Cette technologie (SMS) a un intérêt dans le contexte du courrier électronique pour plusieurs raisons :

- elle ressemble actuellement beaucoup à ce qu'a été le courrier électronique à ses débuts (seulement du texte, par exemple)
- il existe des passerelles entre courrier électronique et SMS (par exemple pour envoyer un courrier électronique sur un téléphone GSM)
- la téléphonie mobile commence à être l'objet de SPAM très similaires à ce qui se rencontre sur Internet

Il y a toutefois une différence considérable : pratiquement dès la mise en service des SMS, on a vu apparaître des SPAM alors que le mouvement a été plus lent pour le courrier électronique. Néanmoins, NTT DoCoMo qui gère au Japon le succès de i-mode, la norme de téléphonie mobile augmentée d'une capacité de communication de données et de navigation web, a dû porter devant la justice les spammeurs qui envahissaient les téléphones de ses clients[24]. En attendant, cette société a commencé à mettre en place les premiers filtres contre le SPAM par messages de type SMS.

SMTP

Simple Mail Transfer Protocol.

Protocole de communication qui permet d'échanger du courrier électronique entre plusieurs machines. On peut le percevoir comme simultanément le service de la Poste et les règles de fonctionnement de la même Poste (mais pour le courrier électronique). Il s'agit d'un des plus anciens protocoles utilisés dans le domaine du courrier électronique.

Aujourd'hui, il est souvent utilisé pour envoyer du courrier (depuis un utilisateur vers un serveur). C'est pourquoi les serveurs SMTP sont souvent les « serveurs de courrier sortant » qui apparaissent dans la configuration des logiciels de messagerie.

Un livre conseillé :

Programming Internet Email

De David Wood

Août 1999

Editions O'Reilly

1-56592-479-7, 378 pages

Ce protocole est très simple de construction, mais il présente une limitation forte : dans la plupart des cas, il ne peut pas accepter directement les lettres accentuées (ou les caractères à 8 bits). Il a donc dû être complété par des moyens de codage spécifiques comme MIME, UUencode, BinHex, etc. Cependant, de plus en plus d'implémentations existent maintenant qui acceptent les caractères à 8 bits.

SMTP online survey

Un site de statistiques qui comparent (en chiffres) les passerelles SMTP les plus courantes sur Internet.

24 En particulier parce que les clients en question payent pour recevoir des messages de type SMS et n'apprécient guère de payer pour recevoir de la publicité.

http://www.bbv.com/SMTP-Survey.htm

Snail mail

Littéralement, *courrier transporté à dos d'escargot*.

Ce terme anglais est très péjoratif et sert à décrire le courrier postal tradionnel pour l'opposer au courrier électronique avec le sous-entendu à peine voilé que le courrier électronique est rapide alors que la Poste (ou son quivalent américain l'US Postal Service) est un service extrêmement lent et probablement peu fiable[25].

A ma connaissance, il ne semble pas y avoir d'équivalent dans la langue française.

SNDMSG

Le nom du programme de gestion locale de messages électroniques que Ray Tomlinson a modifié pour créer le premier système de messagerie électronique au sens où nous l'entendons aujourd'hui.

Une fois modifié il a permis d'envoyer un message de courrier électronique entre deux machines PDP-10 chez Bolt Beranek and Newman (BBN).

Sneakemail

Un service gratuit qui permet de gréer facilement des adresses de courrier électronique jetables. Elles permettent de gérer un peu mieux le SPAM.

Voir adresses jetables.

http://www.sneakemail.com/

Source-routed (ou adresse source-routed)

Il s'agit d'une forme d'adresse de courrier électronique que l'on ne rencontre plus guère aujourd'hui bien qu'elle soit parfaitement valide. Elle a été créée à l'époque où joindre directement toutes les machines d'Internet n'avait rien d'évident. Au contraire, il fallait pratiquement systématiquement faire transiter les courriers électroniques par des machines « intermédiaires » qui ne pouvaient pas forcément être devinées et devaient être indiquées dans l'adresse de courrier électronique.

Ainsi, Pierre%ici.fr@ailleurs.fr est légitime encore aujourd'hui. Cette adresse indique que le courrier est véritablement destiné à Pierre@ici.fr mais qu'il faut d'abord l'adresser à la machine ailleurs.fr qui saura le transmettre à ici.fr.

Cependant, peu de gens rencontreront de nos jours une telle adresse. La mise en place des services DNS a complètement poussé cette pratique à l'obsolescence.

SPAM

On appelle SPAM[26] un courrier électronique non sollicité. Il s'agit le plus souvent d'une publicité commerciale, d'un canular ou d'une tentative d'escroquerie.

Ce type de courrier électronique est rapidement devenu une pratique courante du simple fait de l'avantage financier que représente son emploi pour l'expéditeur : le coût d'expédition de quelques

25 L'escargot peut facilement être victime de ses prédateurs...

26 SPAM est une marque déposée de la société Hormel Foods. C'est la contraction de « spiced ham » (jambon épicé, ce qui est curieux pour un produit qui ne comporte aucun épice). Kenneth Daigneau, acteur et frère d'un dirigeant de Hormel a gagné 100$ en 1936 dans un concours organisé par la firme pour choisir le nom du produit.

millions de SPAM reste tellement faible (au minimum, il n'augmente que très lentement avec la quantité, au point qu'envoyer 1000 courriers électroniques n'est guère plus couteux que d'en envoyer un) qu'il n'est pas utile de chercher à en limiter le nombre par un ciblage.

En conséquence, le SPAM est en phase de devenir un véritable fléau d'Internet et de la messagerie électronique. Certaines études font état d'une moyenne de 1 500 SPAMs reçus par an et par utilisateur du courrier électronique. Cela recouvre une grande disparité de situations, mais a le mérite d'indiquer que recevoir plus de cinq SPAMs par jour n'est pas inhabituel. Cela mène à des évaluations très sérieuses de 10 minutes par jour perdues en moyenne par les travailleurs utilisant le courrier électronique. On parle donc là de sommes considérables perdues par les entreprises du monde entier.

Un brin d'histoire

Initialement, le terme SPAM semble être apparu sur les groupes de discussion Usenet. Il désignait les messages postés en trop grand nombre d'exemplaires ou simultanément dans un trop grand nombre de groupes de discussion. Le terme a été repris pour le courrier électronique dans une acception finalement assez proche.

L'origine du mot lui-même est maintenant considérée comme à peu près sûre (voir Jargon File [1]) : un sketch dans le célèbre show anglais « Monthy Python flying circus » présentait une discussion qui avait lieu dans un restaurant. La serveuse y propose de nombreux plats accompagnés de Spam et un choeur de Vikings répète le mot inlassablement « Spam, Spam, Spam » (pour ceux qui ne connaissent pas les Monty Python, ce genre de situaton invraisemblable est parfaitement normal dans l'univers qu'ils ont développé). Le texte complet du sketch (en anglais, bien sûr) est sur :

http://www.ironworks.com/comedy/python/spam.htm

Le contexte du restaurant rendait la chose d'autant plus amusante que SPAM est la marque anglo-saxonne d'une sorte de jambon en conserve de la société Hormel Foods Corp. qui est souvent considérée à la fois comme de la viande de médiocre qualité et une sorte de symbole légèrement suranné (un peu comme les boîtes de « corned beef » ont longtemps eu en France la détestable réputation qui leur a fait acquérir le titre de « viande de singe »). Mais l'un comme l'autre produit a ses défenseurs acharnés.

Pour fixer des ordres de grandeur des enjeux derrière le SPAM, on retiendra que selon Jupiter Communications, les entreprises dépenseront 7,3 milliards de dollars en publicité par courrier électronique en 2005 (164 millions en 1999). Cela se traduira par le fait que, toujours en 2005, un Américain moyen recevra 1 600 emails publicitaires par an (sur un total de 5 600 courriers électroniques), contre une quarantaine en 1999[27].

Le premier SPAM par courrier électronique semble avoir été produit en 1978 par un responsable marketing de DEC qui a essayé de joindre toutes les adresses du réseau Arpanet de la côte Ouest des Etats-Unis (cela ne s'appelait pas encore Internet). Voici une copie de ce courrier électronique (sans les en-têtes qui faisaient apparaître en clair les nombreuses adresses de destinataires) :

27 Remarquez bien que les chiffres impliquent une utilisation intensive par l'Américain moyen qui tient compte de l'utilisation professionnelle considérable et de celle plus modérée par les autres personnes.

DIGITAL WILL BE GIVING A PRODUCT PRESENTATION OF THE NEWEST MEMBERS OF THE DECSYSTEM-20 FAMILY; THE DECSYSTEM-2020, 2020T, 2060, AND 2060T. THE DECSYSTEM-20 FAMILY OF COMPUTERS HAS EVOLVED FROM THE TENEX OPERATING SYSTEM AND THE DECSYSTEM-10 <PDP-10> COMPUTER ARCHITECTURE. BOTH THE DECSYSTEM-2060T AND 2020T OFFER FULL ARPANET SUPPORT UNDER THE TOPS-20 OPERATING SYSTEM. THE DECSYSTEM-2060 IS AN UPWARD EXTENSION OF THE CURRENT DECSYSTEM 2040 AND 2050 FAMILY. THE DECSYSTEM-2020 IS A NEW LOW END MEMBER OF THE DECSYSTEM-20 FAMILY AND FULLY SOFTWARE COMPATIBLE WITH ALL OF THE OTHER DECSYSTEM-20 MODELS.

WE INVITE YOU TO COME SEE THE 2020 AND HEAR ABOUT THE DECSYSTEM-20 FAMILY AT THE TWO PRODUCT PRESENTATIONS WE WILL BE GIVING IN CALIFORNIA THIS MONTH. THE LOCATIONS WILL BE:

TUESDAY, MAY 9, 1978 - 2 PM
HYATT HOUSE (NEAR THE L.A. AIRPORT)
LOS ANGELES, CA

THURSDAY, MAY 11, 1978 - 2 PM
DUNFEY'S ROYAL COACH
SAN MATEO, CA
(4 MILES SOUTH OF S.F. AIRPORT AT BAYSHORE, RT 101 AND RT 92)

A 2020 WILL BE THERE FOR YOU TO VIEW. ALSO TERMINALS ON-LINE TO OTHER DECSYSTEM-20 SYSTEMS THROUGH THE ARPANET. IF YOU ARE UNABLE TO ATTEND, PLEASE FEEL FREE TO CONTACT THE NEAREST DEC OFFICE FOR MORE INFORMATION ABOUT THE EXCITING DECSYSTEM-20 FAMILY.

Mais, comme indiqué plus haut, le terme SPAM n'a été employé que plus tard et tout spécialement dans le cas de la loterie « green card » exploitée par le cabinet d'avocats américain Canter & Siegel.

Comment arrêter le SPAM :

A ma connaissance, il n'y a aucun moyen infaillible, il n'y a pas de solution absolue. On peut éviter la première apparition du SPAM dans sa boîte-à- lettres en vivant sur Internet comme un paranoïaque, mais c'est beaucoup moins intéressant.

Sinon, vous trouverez des conseils très divers (et à des niveaux de compétence variés) tout au long de cette encyclopédie et dans ses annexes.

Les bénéfices retirés du SPAM :

Il est exact de dire que le SPAM est une activité rentable (et une partie significative de la lutte contre le SPAM consiste justement à réduire ses bénéfices et à rejeter ces comportements du côté des activités mafieuses). Envoyer un million de courriers électroniques ne coûtent que quelques dizaines d'euros. Ce coût immédiat est facile à compenser si seulement quelques destinataires rapportent de l'argent (y compris de petites sommes).

Pourquoi le SPAM est une mauvaise chose :

On pourrait se poser la question de pourquoi ne pas laisser faire. Certains disent bien qu'il suffit de détruire ces courriers électroniques et de les oublier.

En fait, outre le coût considérable du SPAM pour la société (le phénomène a pris une ampleur vraiment étonnante) qui est devenue préoccupante, il fut reconnaître que cette pratique n'a aucune raison de se réguler seule. Le coût unitaire de l'envoi d'un SPAM est ridiculement bas. Le gain potentiel est sans aucune proportion (à condition d'accepter de faire une croix sur les notions d'image de marque ou de réputation).

Contrairement au courrier publicitaire papier (envoyé par la Poste), le coût est tellement faible que l'expéditeur n'a aucun intérêt à limiter la diffusion. Les publicités papier sont généralement *ciblées* (par exemple, un magazine français ne postera pas sa proposition d'abonnement « préférentiel » à tous les américains). Cet équilibre maintenu au niveau de l'expéditeur entre frais et gain potentiel assure une auto-limitation.

Dans le cas du courrier électronique, la plus grande part des frais est payée par le destinataire[28], de manière répartie entre chacun il est vrai. C'est une situation assez proche de n'importe quelle escroquerie où le voleur ne prend qu'une somme mineure à chacune de ses victimes, mais n'en reste pas moins un voleur.

Dans ces conditions, le SPAM n'a aucune raison de se limiter tant que les coûts répartis n'auront pas atteint des montants suffisamment astronomiques pour mettre en danger la totalité de l'édifice Internet. Quel serait l'intérêt d'un Internet sur lequel circulerait majoritairement des propositions plus ou moins alléchantes provenant d'officinces douteuses et parfois franchement mafieuses ?

SpamAnti ou SpamAnti.net

Un des sites qui tentent de lutter contre le SPAM. A la fois par l'information des usagers et par la publication d'une liste noire de domaines qui produisent du SPAM.

http://www.spamanti.net/

NOTE IMPORTANTE : il s'agit d'un site créé et géré directement par l'auteur de cette petite encyclopédie (Yves Roumazeilles, moi !), donc on peut s'attendre à y retrouver certaines des informations présentes ici[29]. Et, on peut supposer que je ne suis pas objectif en le recommandant. Mais c'est quand même - à mon avis - le meilleur site francophone sur le SPAM ;-)

SpamAssassin

Un logiciel écrit en PERL par Simon Cozens pour filtrer le courrier électronique à partir de règles. Il peut être utilisé de diverses manières, mais reste un outil à la convivialité limitée mais compensée par une probable efficacité élevée (je ne l'ai pas testé moi-même).

http://www.perl.com/pub/a/2002/03/06/spam.html

http://spamassassin.taint.org/

SpamBouncer

Logiciel de détection et de filtrage de SPAM réalisé par Michel Bouissou <michel@bouissou.net>.

http://www.bouissou.net/wws/d_read/spamcombat/Spambouncer

Spam Buster

Un logiciel capable de lire directement les messages dans la boîte-à-lettres, de reconnaître certains messages comme étant du SPAM et de les éliminer. Très configurable, ce logiciel est gratuit (mais il affiche de la publicité - sans utiliser une connection Internet pour cela) et peut être payé pour retirer les bannières publicitaires.

http://www.contactplus.com/products/spam/spam.htm

28 Qui de destinataire devient donc une victime d'escroquerie.

29 En particulier, la version la plus récente de l'encyclopédie peut être téléchargée au format électronique PDF directement sur ce site.

SpamCombat

Liste de messagerie francophone traitant du SPAM et du combat contre le SPAM. Elle a été créée et est gérée par Michel Bouissou <michel@bouissou.net>.

http://www.bouissou.net/wws/d_read/spamcombat/

SpamCop

Un service de filtrage de SPAM particulièrement sophistiqué parce qu'il utilise efficacement les déclarations de SPAM faites par les utilisateurs (et un certain nombre de pièges à SPAM) pour identifier l'origine du SPAM. Il a l'avantage d'être essentiellement automatisé, de réagir rapidement à l'apparition d'un nouveau spammeur et de prendre en compte naturellement l'arrêt de ce comportement après quelques jours ou semaines.

SpamCop publie aussi une liste noire de spammeurs pour assister les FAI qui le désirent.

http://www.spamcop.net/

SpamEater Pro

Un logiciel de filtrage spécialisé dans le nettoyage des boîtes-à-lettres de mail. Simple mais puissant.

http://www.hms.com/

Spamford ou Spamford Wallace

Sanford Wallace a acquis dans les années 1990 la réputation d'être un des plus grands spammeurs (il s'était lui-même attribué le titre de « roi du SPAM »). Personnage très arrogant, il a été longtemps la cible principale de toute la communauté anti-SPAM. Cette action a réussi à le contraindre à abondonner cette activité (fin 1998). Il est ensuite revenu (sans grand succés) sur le devant de la scène sous la forme du promoteur d'un marketing plus maîtrisé (excluant le SPAM), avec la société Global Technology Marketing Incorporated (GTMI). Mais sa réputation précédente lui a probablement interdit toute réussite dans ce rôle qui ne lui convenait sans doute pas très bien.

Une curiosité des activités de SPAM de Sanford Wallace est le nombre considérable de noms de domaine qu'il a déposés (ou parfois utilisés sans les déposer). De manière quasiment fanatique, Sanford Wallace a utilisé pratiquement une centaine de noms différents probablement pour éviter d'être identifié et éliminé techniquement par les Fournisseurs d'Accés Internet qui le combattaient.

Parmi les sociétés connues qui ont traîné (avec succès) Sanford Wallace et Cyber Promotions Inc. devant les tribunaux, on peut compter America On Line (AOL), Compuserve (aujourd'hui une filiale d'AOL), Concentric et Prodigy. On notera que Apex Global Information Services (AGIS) a mené un combat particulièrement long contre Sanford et Cyber Promotions, Inc. au moment où ils étaient leur hébergeur. A cette époque, une juge fédérale de Philadelphie (Anita Brody) s'était particulièrement mal fait remarquer en imposant à AGIS de rétablir leur service à Cyber Promotions, Inc. ce qui avait été considéré comme un recul particulièrement douloureux devant le phénomène du SPAM.

Spamhaus

Origine supposée : allemand approximatif ou argotique. Traduction approximative en Français : « maison à SPAM ».

Un Fournisseur d'Accès Internet qui tolère les spammeurs dans ses clients. Un tel FAI est par conséquence souvent listé dans les listes noires, même s'il accueille aussi des clients au comportement plus normal mais qui auront à subir l'ostracisme consécutif aux pratiques malheureuses de leur FAI.

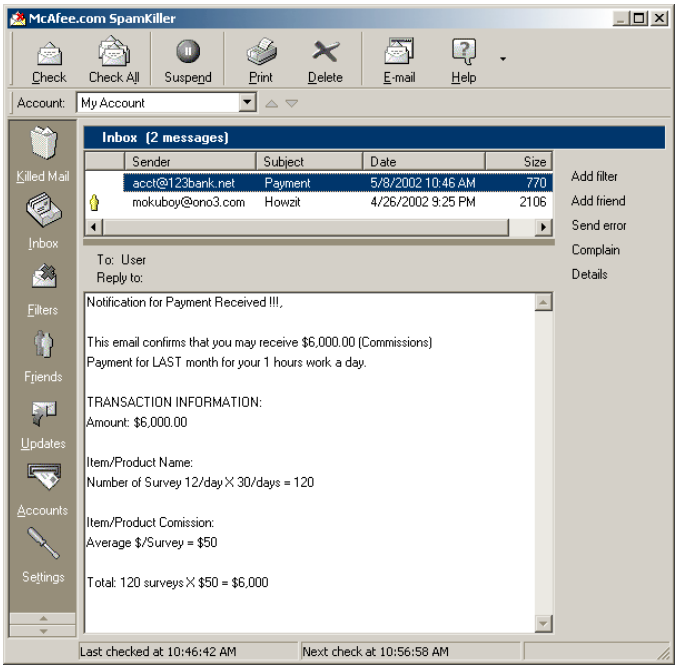
Simultanément, il y a un site www.spamhaus.org qui liste des sites producteurs de SPAM afin de permettre à un internaute de choisir son FAI sans tomber chez un spammeur ou un ami des spammeurs.

Spamhaus project

Ce projet et ce site web (http://www.spamhaus.org/) propose un ensemble de services destinés à faciliter l'identification des spammeurs. Cela passe par *SBL Advisory* (Spamhaus Block List adivsory), une liste d'adresses IP de spammeurs reconnus, de groupes confirmés ou de services de support aux spammeurs ; *ROKSO* (the Register of Known Spam Operations), une liste de spammeurs qui ont été identifiés et chassés plus de trois fois de leur FAI (les 100 spammeurs les plus déterminés de la planète) ; une liste de fournisseurs d'accés ou de connectivité qui abritent un nombre élevé de spammeurs ; une liste de FAIs et d'hébergeurs qui abritent un nombre élevé de spammeurs.

Ces outils sont généralement une excellente base d'informations pour les FAIs eux-mêmes et proviennent directement du Royaume Uni (on peut remarquer quand les européens prennent les choses en main et ne laissent pas faire les seuls américains !).

SpamKiller



Logiciel de filtrage de SPAM (de NovaSoft et maintenant McAfee) qui intervient directement sur la boîte-à-lettres pour en en retirer les messages identifiés comme du SPAM.

http://www.spamkiller.com/

SPAM-L

La principale liste de messagerie consacrée à la lutte contre le SPAM.

Pour vous abonner, envoyez un message à LISTSERV@peach.ease.lsoft.com avec les mots subscribe SPAM-L dans le corps du message.

A cette liste est associée une Foire Aux Questions (http://www.claws-and-paws.com/spam-l/) assez remarquable et complète, même si rédigée en anglais.

spam-list chez schmooze.net

Une liste de messagerie consacrée à la lutte contre le SPAM.

Pour vous abonner, envoyez un message à majordomo@toby.han.de avec les mots subscribe spam-list dans le corps du message.

SpamLaws

Site web réceptacle des décisions, lois et réglements qui contrôlent le SPAM (plus ou moins) dans les différents pays du monde. C'est un site austère de David E. Sorkin, mais il est très utile comme référence légale.

http://www.spamlaws.com/

Spam Motel

Un service qui propose des adresses de courrier électronique « jetables » pour gérer les risques de SPAM.

http://www.spammotel.com/

Spampire

Empire du SPAM. Une société au sommet d'une stratégie de marketing à étage (Multi-Level Marketing) et qui utilise le SPAM pour en assurer la promotion.

SpamWhack

Un service destiné aux Fournisseurs d'Accès Internet qui veulent réduire le risque d'accepter comme client un spammeur. SpamWhack leur fournit un SpamScore (entre 0 et 99) qui permet pour chaque nouvel abonné d'évaluer le risque qu'il soit un spammeur.

La base de données de SpamWhack est alimentée par les FAIs participants, mais le service ne fournit pas les informations concernants les « spammeurs » mais seulement le score résultant des « plaintes » enregistrées (cela assure la confidentialité des informations qui leur sont confiées par les FAIs participants et qui concernent des personnes qui ne souhaiteraient pas voir la tranquilité de leur vie privée ainsi bafouée). Chaque FAI est ensuite libre de choisir les actions à avoir en fonction du score fourni par SpamWhack.

http://www.spamwhack.com/

SparkingWire

Une société qui a décidé de piéger les spammeurs en leur coûtant des efforts pour envoyer des SPAM qui seront systématiquement jetés à la poubelle. Tout courrier qui leur est envoyé est jeté à la poubelle

sans commentaire (pour ne pas utiliser de ressources localement). Il est même renvoyé un accusé de réception si celui-ci est demandé par le spammeur.

Les résultats sont encore à évaluer pour indiquer si oui ou non cela présente (ou peut présenter) un effet nuisible mesurable.

http://www.sparkingwire.com/

Sporge

Un SPAM qui utilise une fausse origine (de « forgery » le mot anglais pour contrefaçon). Le terme semble avoir été inventé par Tilman Hausherr à la suite d'une attaque sur le groupe de discussion Usenet alt.religion.scientology qui utilisait son adresse comme origine apparente (contrefaite).

Richard Stallman

Richard M. Stallman est le fondateur et le coeur battant du projet GNU, l'organisation la plus active du monde du « logiciel libre ». Personnage tout à fait convaincu et charismatique, il est automatiquement associé à ce mouvement dans l'esprit de tous les participants et observateurs.

Statique

Est considéré comme statique une information qui n'évolue pas dans le temps. Dans le cas particulier d'une adresse IP, on peut disposer soit d'une adresse IP statique, soit d'une adresse IP dynamique. Une adresse IP statique est considérée comme généralement préferrable parce qu'elle indique un *lieu* où retrouver une machine de manière immuable.

Summary:

Un en-tête non standard qui est sensé fournir un résumé du contenu du message. Etant donné que très peu de logiciels de messagerie reconnaissent un tel en-tête, il est déconseillé de s'en servir (presqu'aucun destinataire ne saura qu'il y a des informations - éventuellement utiles - dans cet en-tête qui ne lui est pas présenté).

Subject:

Parmi les en-têtes habituels d'un courrier électronique, l'en-tête Subject: est celui qui indique l'objet du courrier. Il s'agit d'une description courte, ou d'un résumé, ou d'un titre qui est entré par le rédacteur du courrier et qui permet habituellement de présenter les courrier de manière simplifiée.

Il est courant de voir un logiciel de messagerie modifier cet en-tête lors de la réponse à un courrier. Par exemple, si un utilisateur répond à un courrier qui contenait l'en-tête

Subject: Pour votre information

La réponse pourra porter en objet

Subject: Re: Pour votre information

Mais, pour éviter les problèmes de lisibilité, il est courant que la réponse à une réponse ne se voit pas augmentée d'un Re: supplémentaire qui donnerait le résultat suivant (rare, mais pas impossible) :

Subject: Re: Re: Pour votre information

On notera qu'il y a des logiciels de messagerie qui ne suivent pas cette règle courante (en particulier, lorsque leur auteur a voulu « franciser » son logiciel). On peut alors rencontrer des variations comme l'emploi du préfixe Ref: ou Réf: ou toute autre possibilité similaire.

Dans le cas où le courrier est « transmis » (en anglais « forwarded »), le logiciel de messagerie pourra utiliser un autre préfixe comme (Fwd).

Subject: (Fwd) Pour votre information

Suffixes de noms de fichiers

Les fichiers attachés et les pièces jointes à un courrier électronique peuvent contenir des vers ou des virus. Plus particulièrement sur Microsoft Windows, certains suffixes de noms de fichiers sont plus souvent vecteurs de virus.

On peut lister des suffixes qui sont susceptibles d'abriter des virus ou des vers :

386, ACE, ACM, ACV, ARC, ARJ, ASD, ASP, AVB, AX, BAT, BIN, BOO, BTM, CAB, CLA, CLASS, CDR, CHM, CMD, CNV, COM, CPL, CPT, CSC, CSS, DLL, DOC, DOT DRV, DVB, DWG, EML, EXE, FON, GMS, GVB, HLP, HTA, HTM, HTML, HTA, HTT, INF, INI, JS, JSE, LNK, MDB, MHT, MHTM, MHTML, MPD, MPP, MPT, MSG, MSI, MSO, NWS, OBD, OBJ, OBT, OBZ, OCX, OFT, OV?, PCI, PIF, PL, PPT, PWZ, POT, PRC, QPW, RAR, SCR, SBF, SH, SHB, SHS, SHTML, SHW, SMM, SYS, TAR.GZ, TD0, TGZ, TT6, TLB, TSK, TSP, VBE, VBS, VBX, VOM, VS?, VWP, VXE, VXD, WBK, WBT, WIZ, WK?, WPC, WPD, WML, WSH, WSC, XML, XLS, XLT, ZIP

Plus spécialement parmi cette liste, on peut citer les suffixes qui ne devraient jamais être acceptés ou exécutés (par exemple, une passerelle de courrier électronique pourrait les refuser systématiquement) :

386, ASP, BAT, BIN, CHM, CMD, COM, DLL, DRV, EXE, FON, HTM, HTML, HTA, HTT, INF, INI, OCX, PIF, SCR, SYS, VBE, VBS, VBX, VXD, WML

Suites mathématiques

Il existe un serveur chez ATT qui permet d'identifier des suites de nombres et de retrouver leurs caractéristiques. Il suffit de lui envoyer un message de courrier électronique avec un contenu comme :

lookup 1 2 5 14 42 132 429 [ne mettez pas de virgule entre les nombres]

Et vous recevrez une identification ou un message avec plus ou moins de détails techniques sur la suite trouvée. Deux adresses peuvent être employées : sequences@research.att.com (pour une recherche dans la base des séquences connues) et superseeker@research.att.com (pour une recherche heuristique qui permettra peut-être de trouver quelque chose de plus profond que les séquences déjà identifiées et archivées).

Supersedes:

En-tête non standard ou Usenet qui désigne la référence d'un article ou d'un message de courrier électronique précédent qui est remplacé par celui-ci. En dehors du contexte Usenet, peu de logiciels de messagerie reconnaissent cet en-tête (même dans le contexte X.400).

Voir aussi Obsoletes:.

3.21. T

Télégraphe

On croit parfois que le SPAM a vu son origine dans le déluge de courrier postal publicitaire qui envahit nos boîte-à-lettres. C'est oublier que l'idée simple (simpliste ?) a pris sa source bien auparavant. J'en ai retrouvé des traces dans le service télégraphique installé par Albert James Myer pour les forces armées américaines aux Etats-Unis dans les années 1870.

Normalement destiné à diffuser des informations de type météorologique, puis utilisé pour des informations plus politiques ou stratégiques (grèves ouvrières ou révoltes indiennes), le service a laissé Myer l'utiliser pour bombarder le Président Grant avec des messages pas tout à fait bienvenus, comme celui envoyé à 3 heures du matin pour annoncer l'arrivée en Angleterre de sa fille Nelly Grant et son mari.

Mais le cas le plus évident est celui de la diffusion par Myer à Grant (quotidiennement en 1873) des prévisions météo pour l'ensemble du pays. Comme il poursuivait le Président jusque dans sa résidence d'été de Long Branch, Myer a fini par recevoir un message laconique mais qui rappelle bien l'énervement de ceux qui recoivent quotidiennement du SPAM dans leur boîte-à-lettres : « Arrêtez ça, Grant (Stop this, Grant) ».

Source : La Recherche - Hors série n° 7, avril 2002 « La météorologie, les Indiens et les grévistes ».

Throwaway account

Un « compte à jeter » qui est ouvert par un spammeur pour envoyer un SPAM. Le compte est considéré comme jetable parce que le spammeur sait qu'il sera fermé par le Fournisseur d'Accès Internet ou le fournisseur de messagerie, mais il le fait en toute connaissance de cause.

Voir aussi drop box.

TiVo

Il s'agit de la marque d'une sorte de magnétoscope numérique (qui enregistre numériquement sur un disque dur) qui a l'avantage de permettre de franchir rapidement (touche « avance rapide ») les publicités d'un programme télévisé.

Mais c'est aussi le produit qui semble avoir lancé en mai 2002 le principe du SPAM télévisé avec l'insertion automatique de programmes promotionnels dans ses menus. Vous n'avez rien demandé et des émissions « sponsorisées » ou « en promotion » viennent s'ajouter à la liste de vos enregistrements. Tout cela étant sans l'avis des utilisateurs, on n'a pas hésité à parler de « SPAM television » en Angleterre (et aux USA).

TLD ou Top-Level Domain

En français : « Domaine du niveau le plus haut ».

Les noms de domaines sont constitués de manière hiérarchique. Ainsi le domaine petit.exemple.fr fait partie du domaine exemple.fr qui fait lui-même partie du domaine fr. On parle de TLD pour les rares domaines qui sont autorisés au niveau le plus haut (fr dans notre petit exemple). Ces TLDs sont gérés exclusivement par l'IANA qui en dresse la liste.

http://www.iana.org/domain-names.htm

Pour connaître le détail des TLD, il est possible de consulter la FAQ (en anglais) « International E-mail accessibility » qui est consultable à http://www.nsrc.org/codes/country-codes.html ou ftp://rtfm.mit.edu:/pub/usenet/news.answers/mail/

On notera qu'il existe plusieurs initiatives isolées de « libéraliser » les TLDs en autorisant la création et l'enregistrement à peu près libre de nouveaux TLD. A ce juor, cela semble sans aucune efficacité pratique, la plupart des logiciels ne tenant aucun compte de ces tentatives.

Ray Tomlinson

Selon Bruno Giussani, Ray Tomlinson a inventé en 1972 le courrier électronique en étendant un système de messages résidant sur une seule machine à un ensemble d'ordinateurs reliés par les premiers développements d'Arpanet, l'ancêtre d'Internet.

Il a ainsi choisi le signe @ pour séparer le nom de l'utilisateur du nom de la machine qui l'acceuille pour la principale raison que c'est un caractère qui ne risquait pas d'apparaître dans ces noms (et donc de créer des confusions). On peut donc penser que la première adresse électronique en réseau fut donc la sienne tomlinson@bbn-tenexa (il n'y avait pas encore de noms de domaines et de gestion DNS qui devait intervenir ultérieurement lorsque l'extension des réseaux l'a imposé).

traceroute

L'outil roi pour l'identification d'une machine. A partir d'une adresse IP ou d'une adresse « en clair », il permet de savoir le chemin que va suivre un paquet IP pour aller de votre machine à cette adresse. En une seule commande il est possible de décoder une adresse, de connaître son fournisseur d'accés et parfois même des indications d'ordre géographique.

On remarquera que cet utilitaire qui est présent sur beaucoup de systèmes d'exploitation, ne porte pas toujours exactement le même nom. Par exemple, sur Windows 98, il s'appelle *tracert*, comme on peut le voir dans l'exemple suivant :

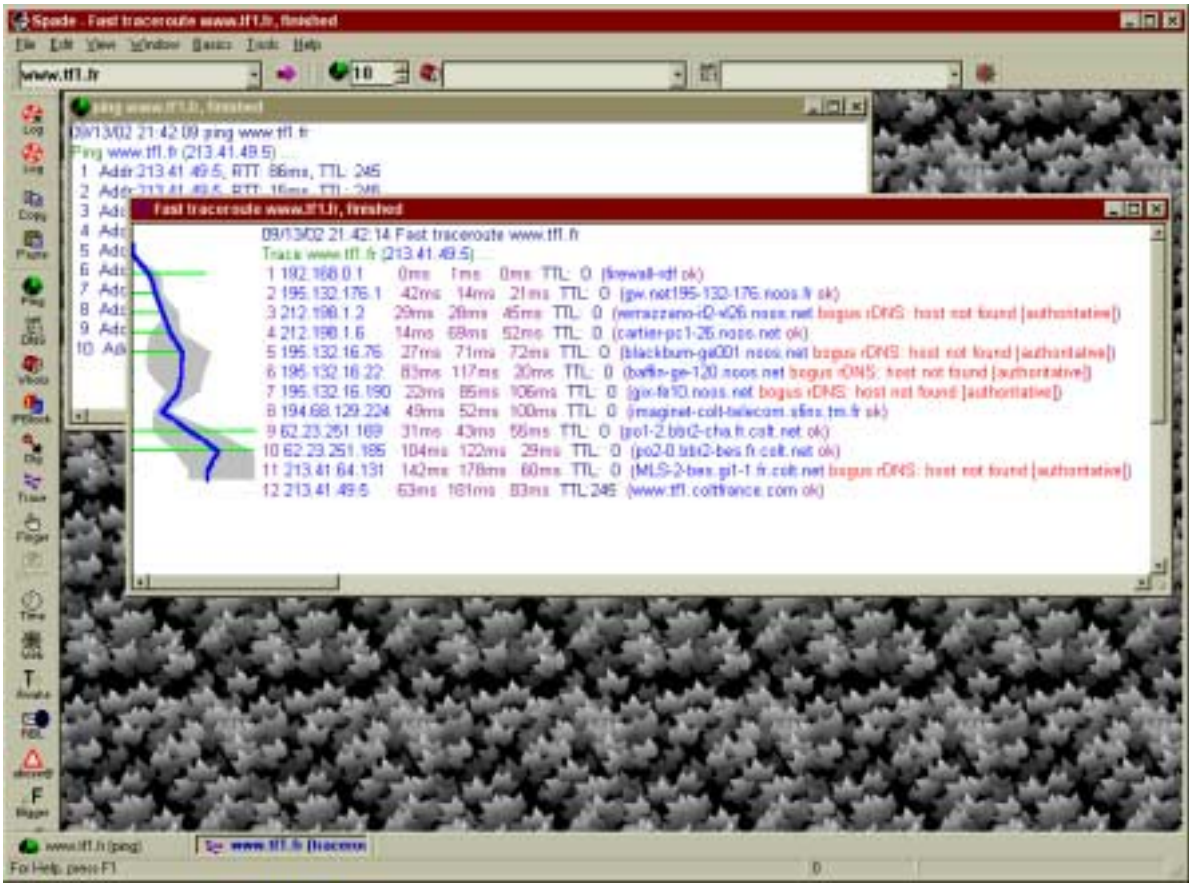
```
D:\USR>tracert www.magic.fr

Détermination de l'itinéraire vers www.magic.fr [195.115.16.3]
avec un maximum de 30 sauts :

  1    1 ms   <10 ms   <10 ms  carotide [192.168.0.1]
  2   36 ms    18 ms    16 ms  gw.dhcp212-198-23.noos.fr [212.198.23.1]
  3   26 ms     8 ms    13 ms  verrazzano-if2-vl26.noos.net [212.198.1.2]
  4   13 ms    11 ms     8 ms  cartier-pc1-26.noos.net [212.198.1.6]
  5  126 ms     8 ms    11 ms  blackburn-ge-030.noos.net [195.132.16.78]
  6   16 ms    10 ms    10 ms  gix-fe10.noos.net [195.132.16.190]
  7   14 ms    10 ms     9 ms  cegetel.sfinx.tm.fr [194.68.129.244]
  8   40 ms     9 ms    14 ms  GammaNC3.esplanade3000.net [195.115.0.134]
  9   55 ms    16 ms    21 ms  CollinesNC1.esplanade3000.net [213.223.0.233]
 10   34 ms    13 ms    16 ms  collines1.esplanade3000.net [213.223.0.229]
 11   18 ms    15 ms    17 ms  gamma1.esplanade3000.net [195.115.0.154]
 12   30 ms    25 ms    14 ms  Magic1.esplanade3000.net [195.115.126.138]
 13   24 ms    65 ms    27 ms  sydney2.magic.fr [195.115.16.230]
 14  155 ms   142 ms   207 ms  www.magic.fr [195.115.16.3]

Itinéraire déterminé.
```

Un exemple de présentation graphique de traceroute généré par Sam Spade serait plutôt :



Voir aussi ping et Sam Spade.

Traduction

Un service gratuit de traduction automatique en ligne (par et pour le courrier électronique) : adressez votre courrier électronique à votre correspondant anglophone et mettez en copie fr_en@t-mail.com ; votre destinataire recevra simultanément la traduction anglaise de la part de t-mail.com. Si vous préferrez l'inverse (anglais vers français), il vous suffit de mettre en copie en_fr@t-mail.com. Simple, non ?

http://www.t-mail.com/

To:

Parmi les en-têtes habituels d'un courrier électronique, on rencontre l'en-tête To: qui désigne le destinataire du courrier. Il est suivi d'une adresse e-mail conforme au RFC 822.

Exemple :

To: info@SpamAnti.net

On peut inscrire plusieurs adresses de courrier électronique sur la ligne To: en les séparant par une virgule.

Exemple :

To: info@SpamAnti.net, John.Doe@stop.abuse.net

Tumbleweed Communications Corp.

Société qui propose des solutions afin d'étendre de manière efficace les notions de confidentialité (au niveau de la société, de ses partenaires ou de ses clients) au niveau du réseau de l'entreprise et donc du courrier électronique.

http://www.tumbleweed.com/

3.22. U

UBE

Unsolicited Bulk E-mail. Plus rarement, Unsolicited Broadcast E-mail.

Terme générique anglais qui décrit le SPAM.

Voir SPAM.

UCE

Unsolicited Commercial E-mail.

Terme générique anglais qui décrit le SPAM. La référence à la caractéristique « commerciale » de ces courriers électroniques est souvent considérée comme un peu trompeuse parce qu'il y a beaucoup de SPAMs qui ne proviennent pas de sociétés commerciales et qu'il y a quelques SPAMs qui ont des intentions moins mercantiles (même si tout aussi ennuyeuses).

Voir SPAM.

UDP (ou IDP)

Usenet Death Penalty ou Internet Death Penalty (en français « peine de mort Internet »).

Décrit la pratique qui consiste à interrompre toutes les communications avec un domaine ou une partie d'Internet au niveau du protocole IP (le plus souvent par une configuration ou une reconfiguration d'un ou plusieurs routeurs). Cette pratique extrême n'intervient que dans des cas extrêmement grave d'abus isolés sur une partie d'Internet où des administrateurs de routeurs ont été suffisamment « agressés » pour en venir à préferrer perdre toute possibilité de communication (web, courrier électronique, FTP, groupes de discussion, etc.) avec le domaine ou le sous-réseau.

Bien qu'IDP apparaisse comme l'acronyme normal de « Internet Death Penalty », UDP est d'un usage plus courant (il signifiait originellement « Usenet Death Penalty » ou « peine de mort Usenet » et ne concernait qu'un isolement Usenet par interruption du protocole NNTP). C'est semble-t-il un exemple de déformation du sens initial d'un vocable pourtant précis.

La sanction d'UDP n'est bien sûr utilisée qu'en dernier recours lorsque la quantité de SPAM reçu par Usenet en provenance d'un FAI donné atteint des proportions ridicules. Toutefois, on peut considérer que cela intervient environ une fois par mois (en ne comptant que les FAIs de taille nationale).

La sanction d'IDP est rarissime. Ses conséquences (l'isolement complet d'un FAI et de ses clients) sont suffisantes pour que cela ne soit appliqué que dans des cas extrêmes, sur des FAI de taille limitée ou sur une partie d'Internet seulement (quelques dizaines de milliers de clients totalement coupés d'Internet ne

constituent pas une situation qui peut être acceptée très longtemps même après échanges d'arguments entre techniciens).

Voir la Usenet Death Penalty FAQ sur http://www.stopspam.org/usenet/faqs/udp.html

Unicode

Un codage de l'écriture utilisable pour à peu près toutes les écritures sur Terre (y compris l'arabe, les caractères chinois, mais qui comporte aussi de nombreux autres jeux de caractères beaucoup moins courants dans le monde).

L'usage du code ASCII ne permet que de décrire les lettres latines de base (de A à Z et de a à z), des chiffres (de 0 à 9) et de quelques signes. Les pays (comme les pays francophones) qui veulent employer des lettres accentuées ont souvent utilisé des extensions du code ASCII. Mais les difficultés rencontrées et la nécessité de trouver une solution adaptée à un environnement global où se croisent des peuples utilisant des alphabets très divers (par exemple, cyrillique ou grec) et des graphies non alphabétiques (comme le chinois) ont poussé à adopter ce codage très riche.

Unicode est certainement appelé à remplacer complètement ASCII comme codage standard. Néanmoins, il faut s'attendre à ce que la transition soit extrêmement longue étant donné le poids de l'existant codé en ASCII et celui des habitudes.

Unix

Famille de logiciels d'exploitation qui a été initialement développée de manière ouverte pour des stations de travail et des mini-ordinateurs et dont les plus récents sous-produits sont dans la famille GNU/Linux.

Upstream ou upstream provider

L'*upstream provider* est le fournisseur de connectivité d'un utilisateur ou d'un domaine. Il s'agit d'une information importante lorsque l'on souhaite porter plainte dans un cas de SPAM : identifier le fournisseur amont permet de trouver à qui se plaindre du comportement d'un utilisateur. Malheureusement, il est parfois difficile d'obtenir cette information à partir des en-têtes d'un message de courrier électronique à cause des techniques de dissimulation utilisées par la plupart des spammeurs.

UUencode / UUdecode

Unix to Unix encoding.

Afin de faciliter le transport de fichiers binaires, il est souhaitable de les « convertir » en ASCII. UUencode est une méthode couramment employée chez les utilisateurs Unix. Néanmoins, le format MIME – plus standard ou plus largement reconnu – remplace peu à peu celle-ci.

3.23. V

VBscript

Cf Outlook.

Vélocipède à anti-propulsion gravitonique de Feynman

Improbable moyen de transport susceptible de révolutionner le déplacement individuel dans les siècles à venir mais sans aucun rapport avec le courrier électronique. En remarquant cette entrée dans l'encyclopédie, vous prouvez qu'il y a donc quelqu'un qui lit cette encyclopédie avec attention... Vous avez toute ma reconnaissance.

Velveeta

Après le succés du terme SPAM, certains ont voulu utiliser cette marque d'une forme de fromage fondu industriel pour désigner la publication d'un même message sur un trop grand nombre de groupes de discussion Usenet (Excessive Cross Posting ou ECP). Le terme est le plus souvent compris, mais n'est plus guère employé.

Voir aussi Jello.

Vers

Logiciel qui se propage en se répliquant de machine en machine. La méthode de propagation n'est pas indiquée dans le nom (on a connu par exemple, le célèbre vers Morris - voir ci-contre - qui s'est répandu sur des machines Unix en utilisant plusieurs moyens dont l'exploitation de bugs de logiciels standard dont certains utilisés par les serveurs de courrier électronique).

On distingue généralement un vers d'un virus par le fait que le vers doit avoir une grande autonomie de fonctionnement et une activité propre qui lui permet de se « reproduire » là où un virus a généralement besoin d'une activité spécifique d'un utilisateur pour se reproduire.

Petit historique

Le 2 novembre 1988, le *vers Morris* (ou *Morris Internet worm*, en anglais) a sans doute été la première occurrence de grande importance d'un vers sur des systèmes informatiques connectés.

En quelques dizaines de minutes, il mettait à mal les machines sur lesquelles il s'installait (généralement, en obligeant l'administrateur à arrêter la machine). On estime qu'il a touché 6 000 machines en quelques jours et les coûts induits cumulés ont été estimés entre 100 000$ et 10 000 000$ par le United States General Accounting Office.

Le vers a été écrit par Robert Tappan Morris, étudiant à Cornell University. Il s'agissait probablement d'une « expérience » qui a dégénéré plus vite que ne le souhaitait son auteur (qui avait déjà procédé à plusieurs expériences mieux contrôlées). R. Morris a été condamné à cinq ans d'emprisonnement et 250 000$ d'amende. Toutefois, sa peine de prison a été commuée en travail d'intérêt général en regard de l'absence de destruction réalisée par son vers.

Pour la petite histoire, Robert Morris était également le fils de Robert Morris Sr., qui était lui-même un expert en sécurité informatique auprès de la National Security Agency (NSA). Cela a mené dans un premier temps à quelques questions sur les motivations réelles de l'auteur.

Cette autonomie d'action est généralement considérée comme un atout important en faveur de la diffusion des vers, mais les capacités propres de la plupart des logiciels informatiques actuels rend cette distinction un peu moins significative puisque la plupart des virus donnent finalement l'impression de se répandre sans assistance (même si cela est techniquement faux, l'impression générale reste).

Dans le contexte du courrier électronique, un vers se propagera – par exemple – en envoyant de lui-même un courrier électronique infecté à tous les individus identifiés dans le carnet d'adresse de l'utilisateur. Le processus pourra ensuite se reproduire chez les nouvelles victimes ainsi désignées.

NOTE : la plupart des distinctions sémantiques indiquées ici sont souvent sujettes à remaniement avec l'évolution de ces « technologies ».

Parmi les vers les plus connus, on remarquera la famile « KLEZ » qui comporte plus d'une dizaine de variantes[30] dont certaines se sont fait remarquer en dissimulant leur origine (le mail infecté semble venir

30 L'une d'entre elle efface totalement le contenu du disque dur de la machine infectée.

d'un correspondant dont le nom et l'adresse ont été « empruntés » dans la carnet d'adresse Outlook Express de la machine infectée. Cette pratique rend très difficile l'éradication de ces vers par la coopération d'utilisateurs n'étant pas capable de lire et comprendre les en-têtes d'un message de courrier électronique (la plupart des utilisateurs, même quand leur logiciel anti-virus a reconnu la présence d'une infection KLEZ dans le courrier reçu, adresse leurs plaintes ou leur information à une personne qui n'est pas l'expéditeur infecté créant une grande confusion, mais ne participant pas ou peu à l'éradication).

Viol de relais

Action qui consiste (dans le cadre de l'envoi d'un SPAM) à exploiter les ressources e-mail d'un serveur de messagerie qui est resté naïvement en configuration open relay.

Le terme de viol est justifié par ce qui est souvent une action très violente (le viol de relais est rarement utilisé pour moins de quelques dizaines de milliers d'envois de messages), sans le consentement de la victime (qui ne prévoyait pas l'abus de ses ressources par un malfaiteur) et qui laisse des séquelles importantes (en particulier par les problèmes récurrents de sécurité et de réparation qui vont généralement suivre l'action initiale).

On observe aujourd'hui dans les statistiques qu'une grande part des serveurs ainsi exploités (avec succés) sont des serveurs du domaine universitaire. Cela provient probablement de leur situation particulière qui fait soit que le « viol de relais » reste non-détecté, soit que les moyens mis en œuvre pour arrêter l'opération sont très faibles.

Vipul's Razor

En français le rasoir de Vipul. Une base de données qui permet de vérifier si un courrier que vous avez reçu a été considéré comme du SPAM par beaucoup d'autres internautes. Cela repose sur l'idée évidente que le SPAM est distribué en quantité ; donc, si les internautes se groupent ils pourront remarquer les SPAM par leur apparition dans plusieurs boîtes-à-lettres (au lieu de la leur seule). Exploité par un outil comme SpamAssassin, cela permet de filtrer le SPAM de manière automatique.

Attention, si les messages qui sont envoyés ne sont pas du SPAM, il est possible « d'empoisonner » Vipul's Razor, mais si beaucoup d'internautes rapportent les incidents de SPAM automatiquement, cela peut devenir terriblement efficace.

http://razor.sourceforge.net/

Virus

Logiciel qui s'installe sur la machine qui est sa cible. Le plus souvent, le virus opère à l'insu de l'utilisateur ou des utilisateurs de la machine. Il est caractérisé par sa capacité à se répliquer et à ré-infecter d'autres ordinateurs par l'intermédiaire de disquettes, de courriers électroniques ou tout autre moyen de propagation qui exploite l'activité de l'ordinateur infecté.

Dans le contexte du courrier électronique, un virus se propagera – par exemple – en infectant un petit logiciel que les utilisateurs s'échangent normalement (par exemple, un fichier attaché exécutable contenant des blagues ou un canular).

NOTE : la plupart des distinctions sémantiques indiquées ici sont souvent sujettes à remaniement avec l'évolution de ces « technologies ».

Historique rapide :

Apparemment, le terme de virus a été « créé » en 1893 par Fred Cohen (alors étudiant à l'Université de la Californie du Sud à Los Angeles - USCLA) en remarquant que les « chevaux de Troie » qu'il observait alors pouvait aussi bien se répandre comme une épidémie à condition de disposer d'un moyen de se reproduire.

Parmi les innombrables virus propagés par e-mail à la fin du vingtième siècle et au début du vingt-et-unième siècle, on notera le LoveBug (ou « I love you ») de mai 2000 semble avoir trouvé sa source à Manille (AMA Computer College)[31] et Melissa qui a acquis une certaine notoriété à son créateur, David Smith, en affectant plus de 100 000 utilisateurs en quelques heures en avril 1999.

Brain, un virus d'origine pakistanaise, fut en 1986 le premier virus à se répandre largement parmi les utilisateurs de PC et à créer des épidémies dans son pays d'origine et à l'Université du Delaware à Newark (en octobre 1987).

Melissa, premier virus de macro Word, s'est initialement répandu à partir d'un document Word paru sur le groupe de discussion Usenet alt.sex qui prétendait fournir une liste de noms et de mots de passe pour accéder à des sites web pornographiques. C'est un excellent exemple de l'assemblage d'un logiciel relativement facile à écrire (en langage de macros Word), de diffusion utilisant les dernières techniques disponibles (le courrier électronique) et une ingéniérie sociale efficace (le sexe reste un attracteur « fatal » pour bien des gens).

Lutte contre les virus et courrier électronique :

La plupart des laboratoires d'analyse des virus disposent d'une adresse de courrier électronique où vous êtes invité à envoyer vos copies de virus (de préférence de virus nouveaux, il n'ont pas besoin de montagnes de copies de vieux virus déjà trop connus).

Laboratoire	*Adresse de courrier électronique*
CAI (IPE), Vet	ipevirus@vet.com.au
Eset (NOD32)	samples@nod32.com
Frisk (F-Prot)	viruslab@f-prot.com
F-Secure	samples@f-secure.com
H+BEDV (AntiVir)	virus@antivir.de
Kaspersky (AVP)	submit-virus@avp.ch
NAI (McAfee)	virus_research@nai.com
Norman	analysis@norman.no
Sophos	support@sophos.com
Symantec (Norton)	avsubmit@symantec.com
Trend	viruslab@trendmicro.fr

31 Sans parvenir à trouver le ou les coupables.

3.24. W

Wanadoo

La branche Internet de France Telecom, l'ancien monopole d'état des télécommunications en France, a une réputation tenace de fragilité dans le domaine du SPAM. Cette réputation semble méritée puisque les incidents attribuables à l'existence d'*open relays* chez Wanadoo se sont multipliés au cours de temps (y compris, en 2001, un épisode comique de confrontation avec Noos où des équipes à la compétence technique insuffisante ont provoqué une escalade verbale et technologique qui a privé ces deux sociétés de leurs échanges de courrier électroniques pendant plusieurs jours).

Comme la plupart des Fournisseurs d'Accés Internet français, Wanadoo semble préférer rester à l'écart des problèmes de SPAM, sans doute ne sachant pas comment apporter une solution même partielle aux problèmes de ses clients).

Web-based e-mail

Certains prestataires de courrier électronique fournissent un service très spécifique qui utilise un accès par le web. Il s'agit de fournir une adresse de courrier électronique (par exemple, yves@hotmail.com) et de s'assurer que tout le courrier qui y est reçu est accessible moyennant l'emploi d'un navigateur traditionnel (Netscape Navigator, Opera ou Internet Explorer). Bien entendu, toutes les autres fonctions du courrier électroniques sont normalement disponibles (réception, envoi, forward, etc.).

C'est très pratique pour plusieurs raisons, mais je voudrais citer les suivantes. Vous n'avez pas besoin de disposer d'une connexion Internet personnelle pour y accéder (il suffit d'emprunter la connexion d'un ami, d'utiliser un web café ou même de lire votre courrier depuis un ordinateur à votre bureau).

De plus, le courrier reste sur le site du prestataire (si vous y accédez depuis le bureau, il n'y aura pas de copie de vos courriers stockés sur le gestionnaire de courrier électronique de votre ordinateur - et cela explique pourquoi certains cabinets de recrutement vous proposent cette prestation).

Ce genre de service se rencontre généralement gratuitement. Le fonctionnement est rentabilisé par la présentation de bandeaux de publicité plus ou moins envahissants sur les pages du site web pendant la consultation de votre courrier.

Je vous signalerai uniquement les suivants :

Nom du service	*Remarques*
USA.net (http://www.usa.net/)	Très stable, très sérieux. Je l'utilise personnellement depuis 1996 (en complément de son service de forwarding).
MSN (http://www.msn.net/)	Service initié par Microsoft.
hotmail.com (http://www.hotmail.com/)	La référence et probablement le plus gros prestataire de ce type.
CJB net (http://www.cjb.net/)	Service de redirection web qui comporte une option de web-mail. Très sérieux.

Le site anglophone http://www.internetemaillist.com/Webbased/ présente utilement un certain nombre de ces services.

On remarquera aussi que certains prestataires vous proposent de relever votre courrier électronique d'une boîte-à-lettres POP3 et de le mettre à votre disposition dans un service à base de web. Ils ne fournissent donc pas (ou seulement en option) une adresse e-mail (vous gardez la votre), mais permettent la consultation de votre courrier électronique (très pratique si vous êtes en déplacement par exemple).

Je vous signalerai uniquement les suivants :

Nom du service	*Remarques*
CJB net (http://www.cjb.net/)	Service de redirection web qui comporte une option de boites-à-lettres POP3 *gratuite*. Très sérieux.
USA.net (http://www.usa.net/)	Très stable, très sérieux. Je l'utilise personnellement depuis 1996 (en complément de son service de forwarding). Le POP3 est un service payant.

Voir aussi Client-serveur.

WebCollector

Un outil de collecte d'adresses de courrier électroniques (un robot) qui a été créé et utilisé par Sanford Wallace dans les années 1990. Il était censé fournir des listes de destinataires organisés en fonction de leurs goûts/intérêts.

Comme l'a dit très franchement Sanford Wallace lui-même : « l'objectif est ici de continuer à fournir aux expéditeurs de courrier en masse les outils dont ils ont besoin pour prospérer dans ce métier particulier. Ce n'est certainement pas de préserver la santé d'esprit (*the sanity*) des destinataires ».

Web collector ne semble plus être observé de nos jours sur Internet depuis la disparition de S. Wallace et Cyber Promotions Inc.

Whack-a-mole

Désigne une activité permanente et quotidienne de tous les administrateurs de Fournisseurs de Messagerie qui consiste à fermer les comptes des spammeurs pour constater qu'ils sont rouverts presqu'immédiatement sous un autre nom. Le terme en anglais approximatif ou argotique fait référence à une mythique chasse à la taupe avec un baton où, chaque fois que le chasseur se précipite sur un trou de taupe et plante le baton dans le trou pour tuer la taupe, il la rate, elle s'échappe et revient pointer son museau hors d'un trou voisin (et ainsi de suite).

Voir aussi SpamWhack.

whois

Ce protocole permet de connaître les informations données par la personne qui a enregistré un nom de domaine. Cela aide parfois à retrouver l'origine d'un spammeur.

De nombreux services whois permettent d'avoir accès à cette information. Je conseille d'utiliser un moteur de recherche comme Google (www.Google.fr) pour retrouver quelques uns de ces sites, ou bien de rentrer le nom de domaine dans un outil comme Sam Spade for Windows.

http://www.whois.net/

Wpoison ou Web Poison

Un outil gratuit qui est utilisé pour construire dynamiquement des pages sur les sites web qui souhaitent « empoisonner » les listes d'adresses collectées par les robots chercheurs d'adresses des spammeurs. Cet outil produit automatiquement des pages web qui contiennent des adresses de courrier électroniques vraisemblables mais purement inventées. L'espoir est de rendre le travail des spammeurs (et de leurs robots) particulièrement difficile.

http://www.monkeys.com/wpoison/

Un outil similaire peut être trouvé sur http://anti.spam.free.fr/, le site français de World Spam Revenge (je le recommande).

3.25. X

X400-Content-Return:

Un en-tête non standard destiné à remplacer Content-Return: et qui permettrait de choisir d'ajouter le corps du message au rapport de non-livraison d'un message (dans le cas où celui-ci n'est pas bien arrivé à son destinataire).

Voir aussi Content-Return:.

X- (en-têtes commençant par)

Les en-têtes dont le nom commence par X- sont considérés comme optionnels. Ils sont souvent seulement informatifs (par exemple, le nom et la version du logiciel qui a servi à la rédaction et à l'envoi du courrier, comme dans le cas d'Outlook Express de Microsoft qui ajoute un en-tête de la forme X-Mailer: Microsoft Outlook Express 5.50.4133.2400). Ils sont parfois utilisés par un seul logiciel ou par une seule classe de logiciel (par exemple, pour « marquer » un courrier électronique dans lequel SpamBouncer a détecté un virus, on pourra trouver un en-tête du type X-SBClass: Virus).

L'encyclopédie liste un certain nombre de ces en-têtes typiquement rencontrés mais ne peut pas se prétendre exhaustive dans ce domaine.

X-Accept-Language:

En-tête optionnel produit par Netscape 6 (version française).

Exemple :

X-Accept-Language: fr-fr

X-Advertisment:

On rencontre parfois dans certains courriers électroniques l'en-tête suivant :

X-Advertisement: TRUE

ou :

X-Advertisement: YES

Il s'agit d'un en-tête parfois utilisé par certains spammeurs souhaitant déclarer leur volonté. Malheureusement, il ne s'agit là ni d'une norme, ni d'un standard de fait.

X-Attachements:

On rencontre parfois dans certains courriers électroniques cet en-tête comme dans l'exemple suivant :

X-Attachements: C:\WINDOWS\TEMP\

X-Beyondmail-Priority:

Cet en-tête optionnel est une tentative de Beyond mail de standardiser les en-têtes de priorité (au moins dans le cadre de leurs propres produits). Les correspondances suivantes soient utilisées :

X-Beyondmail-Priority:	*Signification*
X-Beyondmail-Priority: 3	Priorité maximale (très urgent)
X- Beyondmail -Priority: 2	
X- Beyondmail -Priority: 1	Priorité minimale

Exemple :

X-Beyondmail-Priority: 2

Voir aussi Priority:, X-Priority: et X-MSMail-Priority:.

X-Confirm-Reading-To:

Cet en-tête optionnel est habituellement utilisé par les logiciels de messagerie qui souhaitent recevoir un « accusé de réception » du courrier envoyé. Cette fonctionnalité très diversement supportée par les logiciels existants (certains n'en disposent pas du tout, certains ne l'autorisent que sous condition d'approbation par l'utilisateur, etc.) peut être la source de beaucoup de déception ou de surprises.

Voir aussi X-Rcpt-To: et Return-receipt-to:.

X-Distribution:

Un en-tête spécifique inséré dans les messages rédigés sur Pegasus mail, en réponse à des problèmes de SPAM envoyé par des utilisateurs de Pegasus mail. Quand un message est envoyé à un nombre suffisament élevé de destinataires, Pegasus mail insère automatiquement « X-Distribution: bulk ». Explicitement, cela permet aux destinataires de faire du filtrage actif contre ce type d'envoi.

X-Envelope-To:

Cet en-tête indique à qui est véritablement destiné le message. Il est plus particulièrement utilisé pour indiquer la destination dans un message distribué par une liste de messagerie.

Exemple :

X-Envelope-To: tv8976

X-Errors-To:

Comme Errors-To:, cet en-tête indique une adresse où renvoyer les messages d'erreur. Mais étant optionnel et redondant avec Errors-To:, cet en-tête est peu employé (et rarement reconnu par les serveurs).

X-From_:

Un en-tête optionnel mais tout à fait inhabituel par sa forme (produit par Microsoft Outlook IMO et Lotus/Domino). Son usage semble très mal défini même s'il semble donner une information partiellement redondante avec From:, l'en-tête plus traditionnel.

Exemple :

X-From_: x.dupont@dupont.fr Sun Jun 9 16:54:25 2002

X-Gotcha:

Un en-tête optionnel ajouté par Anomy (un outil de nettoyage/filtrage des messages électroniques pour Linux/Unix).

Exemple :

X-Gotcha: Sanitizer!

X-listname:

Dans le cas de l'envoi d'un message par un logiciel de gestion de liste de messagerie, cet en-tête optionnel peut être utilisé pour désigner la liste et son adresse comme dans l'exemple suivant :

X-listname: <newsletter@spamanti.net>

X-Mail

Logiciel de messagerie électronique conçu pour fonctionner sur Unix (ou Linux ou un autre système d'exploitation proche) sous X-windows (ou une de ses incarnations comme Motif, KDE, etc.)

X-Mailer:

Un certain nombre de logiciels de rédaction de courrier électronique marquent les courriers qu'ils composent avec l'en-tête X-Mailer:. Par exemple, Outlook Express de Microsoft et d'autres ajoutent un en-tête de la forme :

X-Mailer: Microsoft Outlook Express 5.50.4133.2400)
X-Mailer: Lotus Notes Release 5.0.7 March 21, 2001
X-Mailer: The Bat! (v1.52f)
X-Mailer: Pegasus Mail for Win32 (v3.12c)

D'autres logiciels (comme Pegasus Mail) ne produisent aucun en-tête de ce type dans la configuration par défaut sans qu'il s'agisse d'un comportement anormal étant donné que la connaissance de l'outil utilisé pour la rédaction d'un courrier électronique n'est pas censé être nécessaire pour le lire. Le plus souvent, leur utilisateur peut tout de même demander l'insertion de ce type d'en-tête.

X-MimeOLE

En-tête optionnel parfois produit par Microsoft Outlook Express (au moins dans sa version 6.00). Le rôle exact de cet en-tête n'est pas connu.

Exemple :

X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000H

X-MIMETrack:

Cet en-tête optionnel est utilisé pour tracer le parcours d'un mail parmi les serveurs. Il ne semble pas utilisé par autre chose que les serveurs Notes/Domino.

X-MSMail-Priority:

Cet en-tête optionnel est une tentative de Microsoft de standardiser les en-têtes de priorité (au moins dans le cadre des produits Microsoft). Les correspondances suivantes soient utilisées :

X-MSMail-Priority:	*Signification*
X-MSMail-Priority: High	Priorité maximale (très urgent)
X-MSMail-Priority: Normal	
X-MSMail-Priority: Low	Priorité minimale

Exemple :

X-MSMail-Priority: Normal

Microsoft semble avoir adopté la position qui consiste à produire simultanément plusieurs en-têtes de priorité, mais essaye de systématiquement produire cet en-tête qui, bien qu'optionnel, pourrait atteindre le statut de standard de fait pour cette fonctionnalité très mal supportée jusqu'ici par les logiciels de courrier électronique.

Voir aussi Priority: et X-Priority:.

X-Newsreader:

Un en-tête non standard indiquant le type de logiciel de gestion des groupes de discussion Usenet de l'expéditeur.

X-No-Archive:

Cet en-tête est parfois ajouté par certains logiciels de messagerie électronique (principalement des gestionnaires de listes de messagerie). Il est sensé indiquer que le message n'a pas besoin d'être archivé ou sauvegardé (pour des raisons de confidentialité, de respect de la vie privée à long terme, de facilité d'utilisation, etc.)

Exemple (pour indiquer que le message ne doit pas être sauvegardé ou archivé) :

X-No-Archive: yes

X-pmenc:

Cet en-tête n'est produit que par Pegasus mail lors de la création d'un message encrypté par le logiciel lui-même.

Exemple :

X-pmenc: 1.0

X-PMFLAGS:

Cet en-tête optionnel est complètement spécifique au logiciel Pegasus mail. Son contenu est difficile à déchiffrer mais il comporte des informations sur l'emplacement de stockage du message sur disque et un certain nombre d'attributs trouvés dans le contenu du message (par exemple, « le message est-il en format MIME valide ? »).

Comme c'est un en-tête optionnel, il n'est pas reconnu par les autres logiciels de messagerie, mais n'interfère pas avec eux non plus.

X-Priority:

Cet en-tête optionnel permet de donner un niveau de priorité à un message. Il est plus ou moins bien géré, mais le principe veut que les correspondances suivantes soient utilisées :

X-Priority:	*Signification*
X-Priority: 1 (Highest) X-Priority: 1	Priorité maximale (très urgent)
X-Priority: 2 (High) X-Priority: 2	
X-Priority: 3 (Normal) X-Priority: 3	
X-Priority: 4 (Low) X-Priority: 4	
X-Priority: 5 (Lowest) X-Priority: 5	Priorité minimale

Exemple :

X-Priority: 1 (Highest)

On notera en particulier, que les informations de priorité sont rarement traitées pour les petits messages (il est plus simple de les expédier sans aucun traitement de priorité) et quand il n'y a aucun engorgement particulier (le cas le plus courant).

Voir aussi Priority: et X-MSMail-Priority:.

X-Rcpt-To:

Cet en-tête optionnel est habituellement utilisé par les logiciels de messagerie qui souhaitent recevoir un « accusé de réception » du courrier envoyé. Cette fonctionnalité très diversement supportée par les logiciels existants (certains n'en disposent pas du tout, certains ne l'autorisent que sous condition d'approbation par l'utilisateur, etc.) peut être la source de beaucoup de déception ou de surprises.

Voir aussi X-Confirm-Reading-To: et Return-receipt-to:.

X-Sanitizer:

Un en-tête optionnel ajouté par Anomy (un outil de nettoyage/filtrage des messages électroniques pour Linux/Unix).

Exemple :

X-Sanitizer: Gotcha!

X-SpamBouncer:

En-tête optionnel inséré par SpamBouncer dans les messages qui passent par ce gestionnaire de filtres anti SPAM.

Exemple :

X-SpamBouncer: 1.4 MiB (2002/01/07)

X-SBNote:

En-tête optionnel inséré par SpamBouncer dans les messages qui passent par ce gestionnaire de filtres anti SPAM.

Exemple :

X-SBNote: Checking mail using SpamBouncer internal anti-virus module

X-SBRule:

En-tête optionnel inséré par SpamBouncer dans les messages qui passent par ce gestionnaire de filtres anti SPAM.

Par exemple, ceux qui sont reconnus comme portant une pièce jointe exécutable, mais pas forcément reconnaissable par l'utilisateur, reçoivent :

X-SBRule: Hidden Executable

X-SBClass:

En-tête optionnel inséré par SpamBouncer dans les messages qui passent par ce gestionnaire de filtres anti SPAM.

Par exemple, ceux qui sont reconnus comme portant un virus reçoivent :

X-SBClass: Virus

Par exemple, ceux qui sont bloqués comme du SPAM reçoivent :

X-SBClass: Blocked

X-Tagname:

Cet en-tête non-standard est utilisé par Pegasus mail pour marquer certaines formes particulières de courrier électroniques préformatés qu'il peut produire comme un message téléphonique ou une carte de visite électronique.

X-Tagname: PM-TPHONE

X-Tagname: PM-BCARD

X-UIDL:

Un identificateur unique utilisé par le protocole POP3 pour retrouver le message de courrier électronique sur un serveur. Il est normalement ajouté par le serveur de messagerie du destinataire au moment du relevé du courrier par le logiciel client. Il n'y a pas de raison raisonnable courante de voir un message arriver sur un serveur de messagerie avec un champ X-UIDL: déjà rempli. Toutefois, pour des raisons obscures, de nombreux SPAM contiennent cet en-tête dès leur origine.

3.26. Y

Yahoo!

Un fournisseur de messagerie électronique accessible par le web. Très souvent utilisé par les spammeurs comme réceptacle pour créer des drop box (comme de nombreux autres fournisseurs d'adresses gratuites de courrier électronique).

Voir drop box.

You've got mail

Ce film américain de 1998 retrace l'histoire d'amour nouée par courrier électronique entre Tom Hanks et Meg Ryan, deux inconnus qui, dans la vie normale, sont professionnellement et personnellement opposés l'un à l'autre. Le titre provient du message affiché (et parfois clamé par l'ordinateur) quand un abonné AOL reçoit un courrier électronique Le film illustre bien la place prise par le courrier électronique dans la société actuelle.

3.27. Z

Zélotes

Ce terme est parfois utilisé pour décrire les gens qui combattent le SPAM avec beaucoup d'énergie.

ZinCheck

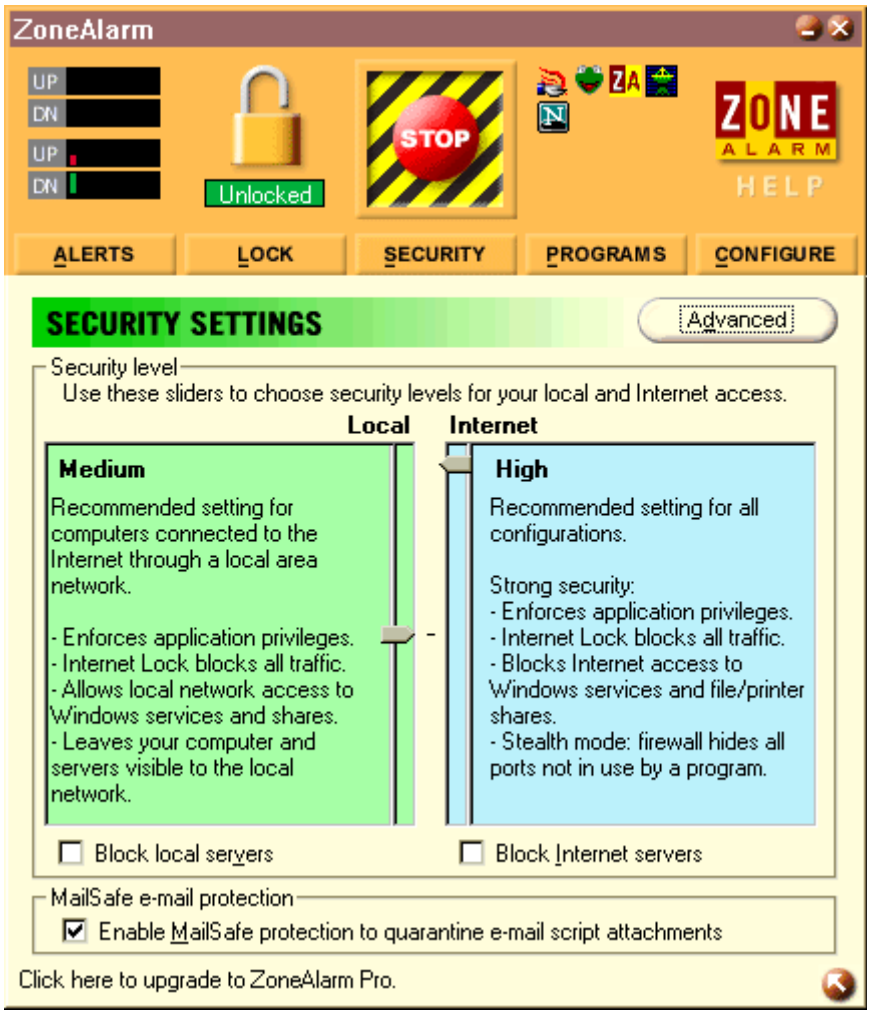
Ce logiciel permet de consulter (sans navigateur) votre (ou vos) boîte(s)-à-lettres sur des prestataires à interface web (web-based). Il reconnaît HotMail, Yahoo!Mail, MailCity, AngelFire et GoPlay. Un complément qui peut se révéler très utile pour leurs utilisateurs.

http://www.zinchak.com/ (il est possible que ce site n'existe plus aujourd'hui)

zmail

Un logiciel client de gestion de courrier électronique développé par Z- Code Software pour X-Windows v11 (X-11).

Zone Alarm



Un excellent logiciel pare-feu (gratuit) sur PC réalisé par Zone Labs. Il existe aussi une version payante plus complète intitulée Zone Alarm Pro.

Ce firewall est significatif ici parce qu'il inclut un outil d'analyse transparente du courrier électronique qui lui permet de reconnaître les pièces jointes à caractère dangereux et de limiter les risques d'exécuter accidentellement une telle pièce jointe qui peut être infectées par un virus : « MailSafe protection ». C'est ainsi un complèment très utile des gestionnaires de courrier électronique (surtout quand ils sont très sensibles à ce genre d'incident comme c'est regrettablement le cas des logiciels de Microsoft).

Ce logiciel n'existe pas encore en version française. Toutefois, une recherche sur le web permet de constater qu'il existe une version (hackée et) traduite en français et une traduction du manuel d'utilisateur. Je ne peux les recommander totalement étant donné leur non-respect des règles habituelles du copyright (en France et ailleurs). Mais le logiciel lui-même est remarquable.

http://www.zonelabs.com/

4. En cas de SPAM : à faire, à ne pas faire

Ne pas attaquer le spammeur. Dans de nombreux cas, les attaques sont dirigées vers une autre victime innocente.

Ne pas répondre à la proposition de désabonnement (remove). Elle ne sert qu'à valider votre adresse en préparation de SPAMs futurs.

Ne pas aider les spammeurs. Eviter de laisser un serveur de messagerie configuré en open relay (il ne doit accepter de transporter des messages que provenant de votre propre organisation).

N'oubliez pas de disposer d'une adresse e-mail spécifique pour ce type de problèmes (abuse@unesociete.fr ou spam@unesociete.be). Vos utilisateurs pourront vous contacter plus facilement, mais surtout, dans le cas où vos serveurs sont victimes d'une attaque de SPAM, il reste un point d'entrée d'information qui n'est pas irrémédiablement pollué par les innombrables messages d'erreur qui vont envahir le traditionnel postmaster@unesociete.fr).

Un livre conseillé :

Removing the Spam: Email Processing and Filtering

De Geoff Mulligan

Avril 1999

Editions Addison-Wesley

0-20137-957-0, 190 pages

4.1. Les meilleurs trucs de la lutte contre le SPAM

Le plus efficace

Les filtres faits sur mesure par vous en fonction des SPAMs que vous recevez. C'est un peu plus compliqué, mais ça finit par être très efficace (au moins au niveau de votre compétence dans la création de ces filtres - qui va aller en s'améliorant avec l'expérience).

Très utile

Des filtres automatiques sont peut-être proposés par votre fournisseur de courrier électronique. Le plus souvent, c'est une option qu'il faut valider volontairement (par exemple, c'est le cas chez USA.net). Ces filtres se veulent aussi efficaces que possible sans jamais perdre un message utile. Par conséquent, en cas de doute, ils préferrent laisser passer le message. Cela donne une efficacité élevée mais laisse passer une part significative de SPAM. Si c'est applicable chez votre Fournisseur de courrier électronique, je vous recommande vivement d'en profiter.

Quasiment inutile

Essayer de se « désabonner » en suivant les liens de type « remove ». Ils ne fonctionnent généralement pas (pour toutes sortes de raisons techniques ou non) et quand ils fonctionnent ils sont souvent utilisés pour enregistrer le fait que votre adresse de courrier électronique existe bien (le problème des listes d'adresses qui sont revendues ici ou là reste qu'elles contiennent beaucoup de vieilles ou fausses adresses. Si un spammeur peut réduire ce taux, il augmente la valeur de la liste – son prix à la revente. En répondant, vous aidez donc les spammeurs à vous spammer).

Inutile

Filtrer les spammeurs individuellement sur l'adresse d'expédition. Cela fait longtemps que les spammeurs n'utilisent plus leur propre adresse en clair. Soit ils créent une boite à lettres pour leur seul envoi, soit ils falsifient le message pour faire croire qu'il provient d'une adresse (vraie ou fausse) qui n'est pas la leur.

4.2. Les activités à risque (relativement au SPAM)

Activités à haut risque

1 - Les listes de messagerie des services commerciaux des entreprises.

On ne peut pas généraliser, mais la pratique de la revente des listes d'adresses (postales ou électroniques) est courante. La chose n'étant pas toujours clairement indiquée sur les formulaires, il est conseillé de rester sur la défensive et/ou d'utiliser une adresse « poubelle » ou une fausse adresse dans les cas où vous ne pouvez éviter de donner votre e-mail mais vous n'avez pas assez confiance.

2 - Certains forums de discussion et de chat, les BBS et quelques listes de messagerie des plus mal gérés.

Soit sur Usenet, soit chez certains prestataires qui en disposent. Si vous ne faites pas très attention, votre adresse de courrier électronique sera publiée soit lors de vos participations, soit tout simplement en vous inscrivant.

3 - Les loteries en ligne, et autre jeux de hasard et d'argent.

Leur laisser votre adresse de courrier électronique est généralement compris comme une invitation à l'utiliser jusqu'à (votre) épuisement et à la revendre à des partenaires plus ou moins sérieux.

Activités à risque modéré mais notable

1 - Enregistrer un nom de domaine

Certains spammeurs collectent les adresses indiquées comme « points de contact » lors de l'enregistrement du nom de domaine, même si ces adresses ne sont jamais utilisées à autre chose.

2 - Les liens e-mail sur un site web

Il existe des robots qui recherchent toutes les adresses de courrier électronique sur tous les sites web qu'ils peuvent rencontrer.

Il existe des moyens techniques divers pour ne pas inscrire cette adresse en clair, mais aucun n'est 100% efficace et ils présentent presque tous un ou plusieurs problèmes d'ergonomie.

Activités quasiment anodines

1 - Faire des achats sur Internet.

Vous recevrez sans doute les offres promotionnelles de la société qui vous a vendu des bouteilles de vin, des livres, des disques ou un ordinateur. Mais il est aujourd'hui très courant que ces sociétés s'attachent à gérer correctement votre adresse (entendez « sans en abuser, ni la revendre »). Il y a des exceptions, mais la dernière des choses à faire commercialement parlant est de fâcher un client existant. Il est déjà à 50% un client futur, et il coûte moins cher à convaincre de rester et de renouveller ses achats que de trouver un nouveau client.

2 - Ouvrir un compte e-mail gratuit.

Il ne semble pas y avoir de cas où la seule ouverture d'un compte génère du SPAM. Les prestataires de courrier électronique (même gratuit) ne revendent tout simplement pas votre adresse.

3 - L'enregistrement d'un logiciel freeware

Les créateurs de freeware ne semblent pas non plus avoir ce genre d'envie. Probablement, ne sont-ils pas tentés par la petite rémunération que la vente d'adresses leur rapporterait (ou alors ils vendraient le même logiciel en shareware pour un bénéfice supérieur).

4 - L'inscription sur une lettre d'information (ou newsletter)

Sauf cas accidentel, votre adresse de courrier électronique est tenue secrète. Vous recevrez un volume plus ou moins important d'e-mails, mais n'est-ce pas justement là l'idée de la lettre d'information.

5 - L'enregistrement en ligne d'un logiciel

Le vendeur demande parfois l'adresse de courrier électronique de l'acheteur pour valider l'enregistrement en ligne. Mais cela ne semble pas produire de SPAM (et souvent même aucun courrier électronique de la part de la société vendeuse).

4.3. Techniques de détection (pour un utilisateur)

Il s'agit de reconnaître les en-têtes de SPAM tels qu'ils apparaissent à l'arrivée dans la boîte-à-lettres. Donc, ces techniques sont accessibles à un utilisateur normal (contrairement à ce qui sera présenté un peu plus bas et qui ne peut s'appliquer qu'à un Fournisseur d'Accès Internet).

Tous comptes faits, il y a certaines marques très spécifiques du SPAM que l'on peut rechercher dans le courrier électronique en vue de sa « classification ». J'ai moi-même relevé quelques en-têtes très particuliers.

Vous pouvez utiliser cette information pour faire du tri ou du filtrage. Toutefois, n'oubliez jamais qu'il peut s'être glissé quelques erreurs dans mon travail. Il convient donc de bien tester avant de mettre en service un outil de filtrage.

Remarque pour le spammeur apprenti qui penserait à utiliser les informations présentent ici pour trouver un logiciel l'aidant à spammer : Si je liste ici un logiciel, c'est qu'il s'agit sans doute d'un des moins « efficaces ». Cela n'est donc même pas la peine d'aller acheter ou downloader un de ces logiciels qui seront arrêtés par les filtres qui sont mis en place de manière de plus en plus systématique.

Authenticated sender

On rencontre parfois (en 2002, cela commence à être moins courant) dans certains courriers électroniques l'en-tête suivant :

```
Comments: Authenticated sender is [un nom ou une adresse]
```

Je n'ai toujours pas réussi à identifier le nom exact du logiciel de SPAM qui introduit cet en-tête[32], mais c'est un des marqueurs les plus efficaces jamais rencontré en matière de détection de SPAM.

32 Si vous pouvez m'indiquer l'origine exacte, je vous en serai reconnaissant.

X-Mailer:

Un bon nombre de logiciel de SPAM signent clairement leurs envois. Je vous présente ci-après une liste d'en-têtes de type X-Mailer que produisent des logiciels d'envoi de SPAM.

X-Mailer: : Microsoft Outlook Express 6.00.2600.0000
X-Mailer: <Mailcast, version 1.0>
X-Mailer: AOMail 6.4
X-Mailer: Atlas Mailer 1.0
X-Mailer: Aureate Group Mail Free Edition - http://software.aureate.com
X-Mailer: Campaign Manager v2.0 http://www.portalofone.com
X-Mailer: DMailer for Windows V1.1
X-Mailer: GOTO Software Sarbacane Vs 1.10C[33]
X-Mailer: GOTO Software Sarbacane Vs P1.13b
X-Mailer: JumboMailer 1.01
X-Mailer: MailExpress Lite
X-Mailer: MailWorkZ Version 4.3.1
X-Mailer: MaxBulk Mailer v1.7.4
X-Mailer: Outlook Express
X-Mailer: outlook express
X-Mailer: UnityMail
X-Mailer: Unknown (No Version)
X-Mailer: MAGIC
X-Mailer: Mail bomber
X-Mailer: Mail expeditor
X-Mailer: Dynamic Opt-In Emailer
X-Mailer: EMAILCOLLECTORPRO
X-Mailer: Prospect Mailer 2000
X-Mailer: WC Mail

Si vous êtes attentifs, vous aurez remarqué certains en-têtes qui pourraient laisser penser que le mailer est un logiciel d'origine respectable. Il y a donc des en-têtes falsifiés pour ressembler à ceux de Microsoft Outlook Express ou d'AOL. Les différences sont mineures, mais reconnaissables (faute de frappe, description incomplète et non-conforme aux standard de l'original).

Par ailleurs, certains des fabricants de ces logiciels affirmeront sans doute que leur logiciel n'est pas destiné à produire du SPAM mais seulement du courrier en masse. Je vous conseille donc d'envisager la possibilité de perdre les messages envoyés par un diffuseur « utile » si vous filtrez ces marqueurs. Toutefois, dans mon expérience, ces en-têtes X-Mailer: ne se rencontrent que pour du SPAM et sont des indicateurs très fiables du caractère de SPAM d'un courrier électronique.

33 Potentiellement, Sarbacane n'est pas seulement un logiciel de SPAM, mais je n'ai encore pas observé de message qui soient envoyé par Sarbacane sans être du SPAM.

From:

Quelques SPAMs sont clairement identifiables par l'origine affichée (c'est rare, mais on peut en trouver quelques uns). Je signalerais seulement un cas (lié à un virus plus qu'à un SPAM, d'ailleurs) :

From: hahaha@sexyfun.net

Il s'agit d'un moyen de reconnaissance du virus « Blanche Neige ».

Je ne donnerai pas d'adresses. Je vous conseille plutôt de collecter votre propre petite liste tout en gardant à l'esprit que la très grande majorité des From: sont falsifiés dans le cas des SPAMs.

Sinon, vous pouvez refuser tous les mails dont le domaine listé dans From:, Reply-To:, Sender: ou Return-Path: est aussi présent dans la liste noire de SpamAnti (http://www.spamanti.net/).

En-têtes MIME

Certains coupables se reconnaissent plutôt aux marques qu'ils laissent dans la construction de messages de type MIME.

JumboMailer est visible à cause de l'en-tête :

MIME-Engine: JumboMailer 1.01

KingMailer est détectable à cause des « boundary » de type MIME qui portent son nom. On peut alors voir soit la déclaration de « boundary » soit l'utilisation :

Content-Type: multipart/alternative; boundary="___KingMailer_Alternative_1964_asbhsdjhglwKM___"
--___KingMailer_Alternative_1964_asbhsdjhglwKM___--
--___KingMailer_Related_1964_asbhsdjhglwKM___--

Chacun choisira la meilleure expression pour reconnaître ces « marqueurs ».

Autres

Je peux ensuite confirmer que les SPAMs envoyés par Aureate Group Mail Free Edition comportent toujours l'URL du site web où on peut le télécharger (http://www.group-mail.com). C'est le concepteur lui-même qui le dit. Autrefois, le site était http://software.aureate.com .

Un autre logiciel de SPAM semble utiliser avec constance le champ To: avec une adresse Friend@public.com. C'est assez curieux parce que j'aurais d'abord pensé que c'est une adresse saisie au hasard par un spammeur en mal d'idées. Sauf que cela se reproduit avec acharnement depuis plusieurs années. Ce qui en fait un des bons « détecteurs » de SPAM.

To: Friend@public.com

J'ajouterais que je crois que dans ce cas le Message-ID: est systématiquement vide comme :

Message-ID: < >

J'ai encore repéré un logiciel de SPAM qui indique son nom dans le champ User-Agent: plutôt que dans le X-Mailer: ; donc, pas très différent en principe, mais aisé à détecter.

User-Agent: MaxBulk Mailer/v0.11d

Enfin, une marque du spammeur bête qui utilise un logiciel de SPAM qu'il n'a même pas payé[34] est l'apparition en début de message (dans le corps du message) du texte suivant :

This message was transferred with a trial version of CommuniGate(tm) Pro

Note : ce texte peut avoir quelques caractères supplémentaires en début ou en fin de ligne, mais il tient toujours en une seule ligne de texte.

4.4. Techniques de détection (pour un FAI)

Certaines techniques de détection du SPAM peuvent être employées par un Fournisseur d'Accès Internet ou un serveur de mail (un MTA). Il s'agit de conseils qui n'intéresseront que les administrateurs de messagerie avec un minimum de connaissances sur le sujet, mais je crois qu'il est utile de prendre le temps de les comprendre si vous êtes un administrateur (cela fera progresser grandement votre compréhension du courrier électronique).

« Junk Mail Detection » (http://www.lyris.com/mshelp/JunkMailDetection.html) présente la plupart d'entre elles en anglais[35], mais je vous fournis quelques éléments de base.

Vous allez vite remarquer qu'il s'agit de refuser les courriers électroniques et les connexions SMTP qui contiennent des informations invalides, mal formées, impossibles, anormales ou tout simplement falsifiées. Moins il circulera de choses anormales par vos serveurs mieux tout le monde se portera (et vous en premier, bien sûr).

Listes de connexions dial-up

Utiliser les DUL pour bloquer des courriers qui sont très probablement illégitimes (voir article DUL).

Taille du HELO

Il y a (ou a eu) dans sendmail un bug qui permettait à un utilisateur de ce programme de ne pas faire apparaître son adresse IP dans les messages qu'il faisait envoyer. Pour cela il suffisait d'avoir une ligne HELO (dans le protocole SMTP) suffisamment longue pour faire déborder un buffer interne.

Tout message dans lequel le nom d'une machine apparaissant sur une ligne Received: est exagérément long (plusieurs centaines de caractères) est probablement le signe d'une tentative (éventuellement

34 A mon avis, cette mesquinerie financière de la part d'assez nombreux spammeurs donne une idée de leur honnêteté et des mauvaises intentions qu'ils ont quand ils commencent à envahir nos boîtes-à-lettres. Ne vous attendez pas à ce qu'un tel personnage respecte son engagement de vous retirer de sa liste de messagerie, ou de préserver votre vie privée, s'il ne peut pas s'empêcher d'économiser quelques dizaines de dollars pour envoyer son message publicitaire. A mon avis, ce n'est plus du commerce, mais du mercantilisme malhonnête.

35 Cette page décrit en fait des techniques qui sont implémentées dans MailShield, un MTA particulièrement protégé contre les incidents de type SPAM, mauvaises configurations d'autres serveurs et tentatives d'intrusion utilisant le courrier électronique.

réussie) de dissimuler l'origine du SPAM. Il est en effet rare de rencontrer des machines dont le nom soit si long qu'il tombe dans la catégorie « plus de 200 carcatères » !

RBL et RSS

Utiliser les listes RBL (voir article RBL). Elles indiquent en temps réel si une machine fonctionne comme un « open relay » (et se trouve donc pouvoir devenir à tout moment un diffuseur de SPAM).

Refuser les MAIL FROM vides ou invalides

C'est une pratique légitimée par les RFC que de diffuser des messages dont les MAIL FROM sont vides (et cela est utilisé par certains logiciels de gestion de listes de messagerie un peu anciens), mais c'est aussi une pratique courante de spammeurs qui ne souhaitent pas diffuser leur adresse.

Eventuellement, on peut limiter ce contrôle aux messages qui s'adressent à des destinataires multiples (To: avec une liste de destinataires).

Globalement, il s'agit d'un choix difficile pour la plupart des administrateurs parce qu'il peut mener au refus de (rares) courriers électroniques légitimes.

Plus sûr est le contrôle de la validité de l'adresse de courrier électronique qui est présentée dans le MAIL FROM (pour cela on pourra se référer utilement à une expression régulière comme celle présentée au chapitre 9.1).

Refuser les Date: erronnées ou invalides

Pour des raisons que je ne comprends toujours pas, certains logiciels de SPAM et certains spammeurs produisent des dates de messages absolument ridicules. Soit il s'agit de pousser le message en tête de la liste des messages reçus (pour cela on trouve des dates en avance de quelques jours sur la date courante), soit il s'agit d'en-têtes Date: non conformes aux règles imposées par les RFC.

Ce filtrage ne semble pas poser de problème et ne relever que des spammeurs (mais souvenez-vous d'accepter les messages dont les dates sont très anciennes, parce qu'ils peuvent résulter d'une erreur de configuration, d'une panne d'horloge ou de mémoire non-volatile sur l'ordinateur de quelqu'un qui ne s'en est pas encore rendu compte).

Refuser les From: et les To: erronnés ou invalides

Les en-têtes From: et To: doivent contenir une adresse de courrier électronique valide. Il est donc utile de refuser les messages qui ne s'y conforment pas (il s'agit généralement de dissimulation de l'origine du courrier, une pratique de spammeur par trop courante).

Exemples de ligne To: valides :

```
To: info@SpamAnti.net
To: "Yves Roumazeilles à SPAM.Anti!" <info@SpamAnti.net>
```

Exemples de ligne To: à refuser :

```
To: Tom
To: "E-mail marketing Co." <SPAM@Email.Marketing>
```

Le premier contient un texte qui ne peut pas être confondu avec une adresse, le second est un petit peu plus subtil puisqu'il faut remarquer que Email.Marketing ne peut pas être une adresse de courrier

électronique valide (pour cela on pourra se référer utilement à une expression régulière comme celle présentée au chapitre 9.1).

Refuser les adresses « source-routed »

Voir l'article « source-routed » pour plus de détails. Ces adresses sont légitimes, mais tellement anormales de nos jours qu'on ne les rencontrent plus que dans des cas de tentatives de manipulation.

Contrôler le respect des standard Internet

Il s'agit d'une prophylaxie minimale. Elle a l'avantage d'éviter de nombreux problèmes qui ne sont pas tous liés au SPAM, mais il existe un nombre considérable de contrôles qui peuvent être faits sur un message de courrier électronique et qui permettent de détecter soit une erreur de configuration, soit une tentative de fraude. Pensez à vous assurer de la présence des en-têtes obligatoires (Date:, To:, From:, Subject:, etc.) et à surveiller très précisément l'information fournie dans les champs MAIL FROM ou HELO d'une connexion SMTP (pour les serveurs eux-mêmes).

Imposer des limites raisonnables

Si vous êtes un FAI (ou même une entreprise qui gère son propre serveur de courrier électronique), il peut être utile de fixer une politique de limites applicables au courrier électronique : limiter la taille des messages, le nombre de destinataires, etc.

Le choix des valeurs limites est une décision importante pour ne pas handicapper vos utilisateurs, mais une sécurité notable. Cette décision ne doit pourtant pas être gravée dans le marbre : n'oubliez pas que vos utilisateurs voient leurs habitudes changer au fur et à mesure de leur acquisition de connaissances et des développements de la technique.

Interdire le fonctionnement en « open relay »

Ce mode de fonctionnement (voir les articles relais et open relay) n'est jamais souhaitable[36]. Si vos serveurs de messagerie doivent pouvoir s'aider mutuellement, prévoyez une liste des serveurs pour lesquels vous aceptez de faire du relais de courrier (vous pouvez avoir une structure interne à plusieurs serveurs, par filiale, par service, etc.), mais ne laissez pas « n'importe qui » utiliser vos ressources. Les spammeurs en profiteront à vos dépens.

36 Dans certains cas, on souhaite avoir temporairement un système configuré en « open relay » afin de faciliter la mise au point ou le déploiement d'un réseau. Dans ce cas, il est important de ne pas laisser les machines dans cette configuration. En effet, les robots qui cherchent à identifier ce genre de situation pour l'exploiter ne se précipiteront probablement pas en seulement quelques heures pour procéder à un viol de relais, mais un oubli peut se traduire par des incidents très désagréables.

5. Extraction des en-têtes

La quasi-totalité des logiciels de messagerie électronique dissimulent la plus grande partie des en-têtes (qui ne sont normalement pas nécessaires à l'utilisateur). Toutefois, soit pour déterminer l'origine exacte d'un message abimé ou falsifié, soit pour dépanner un problème de courrier électronique, on peut être amené à tenter de visualiser les en-têtes complets d'un message.

Je donne ici la procédure pour certains logiciels.

5.1. Outlook Express 4

Ouvrez le message ; dans le menu Fichier, sélectionnez Propriétés, puis Détails.

5.2. Outlook Express 5

Quand on a ouvert un message, il suffit de d'appeler le menu Fichier>Propriétés... et de cliquer sur l'onglet Détails.

Eventuellement, on appréciera de cliquer sur le bouton Source du message... si l'on souhaite obtenir une copie des en-têtes.

Si le message n'est pas ouvert, il suffit de le sélectionner dans le panneau de messages, d'utiliser le click droit de la souris pour obtenir le menu contextuel dans lequel on choisira l'option Propriétés... pour retrouver les mêmes boites de dialogue qe ci-dessus.

5.3. Outlook Express for Macintosh (version anglaise)

Quand le message est sélectionné, choisir le menu View>Source. La fenêtre qui apparaît présente le courrier électronique complet avec tous ses en-têtes originaux.

5.4. Outlook (fourni avec Microsoft Office)

Faites un clic droit sur le mail voulu puis choisissez Options. Dans la fenêtre qui s'ouvre, dans un cadre spécifique en bas de la fenêtre, copiez l'en-tête complet : « Received from... » jusqu'à « Content-type... ». Créez ensuite le mail envoyer et faites un clic droit pour « Coller » l'en-tête dans le corps du message, là où vous souhaitez l'insérer.

5.5. Pegasus mail v3.x

Quand un message est affiché, il suffit de cliquer sur le texte du message avec le clic droit de la souris pour voir apparaître un menu contextuel dans lequel on peut choisir l'option « show raw message data ». Le raccourci clavier équivalent est Ctrl-H.

Note : quand un message est affiché avec tous ses en-têtes, ils sont automatiquement inclus avec les autres en-têtes dans une réponse ou un forward.

5.6. Pegasus mail v4.x

Ayant ouvert un message de courrier électronique dans Pegasus mail (par exemple en double-cliquant dessus), il suffit de cliquer sur l'onglet « raw view » pour faire apparaître l'ensemble des en-têtes.

Dans tous les cas, pour envoyer les en-têtes complets à un correspondant (par exemple dans le cas d'une plainte pour SPAM), il suffit d'utiliser la commande « forward » et de sélectionner la méthode de forwarding « Start a new message with the messages attached » qui incluera complètement le message original.

5.7. Netscape mail réçent

Dans la fenêtre Mail, sélectionner View, puis Page Source. Ctrl-U est le raccourci clavier correspondant.

5.8. Netscape mail v3.x

Dans la fenêtre Mail, sélectionner Options, puis Show Headers, et ensuite Full.

5.9. Eudora Light

Sélectionner Special et puis Settings, ou selectionner Tools et puis Options, selon la version. Parmi les icônes à gauche dans la fenêtre de dialogue, sélectionner « Fonts and Display », puis cocher « Show all headers (even the ugly ones) ».

Sur certaines versions 3 et 4, il y a un bouton « Blah » sur le message. Il suffit de cliquer ce bouton.

5.10. Claris E-mailer

Sélectionner le menu Mail et puis « Show long headers ».

5.11. HotMail

Cliquer sur « Options » dans la barre de navigation à gauche de la page. Puis cliquer sur « Préférences ». Il suffit ensuite de sélectionner « Message headers : full ».

5.12. KDE mail

Sélectionner View, puis « All headers ».

5.13. Information complémentaire

Malheureusement en anglais, le site web de SpamCop fournit aussi des informations détaillées pour un nombre important de logiciels qui ne sont peut-être pas indiqués ici.

http://spamcop.net/fom-serve/cache/19.html

Quelques endroits où vous pourrez trouver encore plus de détails (en anglais et avec des copies d 'écran) :

http://www.wurd.com/eng/ABCs/ms_headers.htm - MS Outlook Express et Internet Mail

http://www.wurd.com/eng/ABCs/mac_headers.htm - MS Outlook Express pour Mac

http://www.wurd.com/eng/ABCs/ns_headers.htm - Netscape Messenger et Netscape Mail

Certains programmes qui ne sont pas vraiment compatibles avec Internet détruisent ces en-têtes critiques. On peut citer dans cette catégorie : cc-Mail, Beyond Mail, VAX VMS. Ne cherchez pas. Pour eux, récupérer tous les en-têtes est sans espoir. Utilisez un autre logiciel de messagerie pour cela.

Quelques URL pour vous aider (en anglais) :

http://support.xo.com/abuse/guide/guide1.shtml

http://ddi.digital.net/~gandalf/trachead.html

http://www.fmp.com/spam_patrol/tracking.html

6. Comprendre les en-têtes de courrier électronique

Pour véritablement comprendre comment fonctionnent les en-têtes de courrier électronique, je n'ai malheureusement pas de solution miracle. Il faut d'abord lire les RFC correspondants, puis observer les messages que l'on reçoit, puis observer les messages de spammeurs, puis comprendre comment ils trichent avec les en-têtes. Et ensuite, on peut commencer à comprendre des choses qui ne sont pas toutes évidentes.

Bon, OK ! Vous voulez quand même une solution rapide. Alors, voici des éléments que j'ai essayé de rassembler sous la forme d'un exemple détaillé.

6.1. Retrouver l'origine d'un SPAM

C'est rarement très facile pour deux raisons principales :

- l'origine d'un mail n'est pas très facile à déterminer dans le cas général,
- les spammeurs tentent souvent de dissimuler l'origine de leurs activités.

La première chose à faire est de consulter les en-têtes complets du message à explorer. La plupart des logiciels de messagerie présentent des informations qui sont très faciles à falsifier (`To:`, `From:`, etc.). Seules les lignes `Received:` (qui ne sont le plus souvent accessible que par l'intermédiaire d'une commande séparée de votre logiciel de messagerie) sont vraiment difficiles à trafiquer.

Le chapitre précédent donne des conseils détaillés sur comment afficher les en-têtes complets d'un message (en fonction de votre logiciel de courrier électronique).

6.2. Décoder les en-têtes Received:

De manière générale, un en-tête `Received:` raisonablement récent et convenablement conforme aux habitudes les plus courantes pourra ressembler à :

```
Received: from host1 (host2 [xx.xx.xx.xx]) by host3 (6.5.007)
      id 3CD2B91F0014E764 for nom@domaine.fr; Mon, 6 May 2002
21:28:59 +0200
```

On y trouve des informations importantes comme :

- host1 : la machine qui a envoyé le mail,
- host2 [xx.xx.xx.xx] : son adresse IP, et éventuellement le reverse-DNS de cette adresse,
- host3 : la machine qui l'a reçu et a ajouté la ligne `Received:`,
- nom@domaine.fr : le destinataire reconnu par host2.

Le format va varier d'une machine à l'autre, mais il est important de comprendre que chaque machine qui voit transiter le message va ajouter une ou plusieurs lignes de type `Received:`.

Les plus récentes sont en haut du message. Les plus anciennes (et celles qui sont le plus probablement fausses) sont en bas de la liste.

Voici un exemple de SPAM que j'ai reçu sur une de mes adresses de courrier électronique et le suivi détaillé des opérations de décodage que l'on peut réaliser. J'espère que cela vous aidera à mieux comprendre.


```
Received:  from cmsmail08 [127.0.0.1] by cmsmail08 via mtad
(CM.1201.1.04A) with ESMTP id 888gecJI81094M08; Fri, 03 May 2002
09:34:59 GMT
Received: from baro.antw.online.be [62.112.0.23] by cmsmail08 via smtad
(CM.1201.1.04); Fri, 03 May 2002 09:34:59 GMT
Received: from server_pdc.aspaburo.be (gateway.aspaburo.be
[194.88.105.138]) by baro.antw.online.be (8.9.3/8.9.3) with ESMTP id
LAA35553; Fri, 3 May 2002 11:29:50 0200 (CEST)
Message-Id: <200205030929.LAA35553@baro.antw.online.be>
Received: from smtp0351.mail.yahoo.com (mail.elsystravel.com
[66.12.138.26]) by server_pdc.aspaburo.be with SMTP (Microsoft
Exchange Internet Mail Service Version 5.5.2650.21) id JHNSAL6F; Fri, 3
May 2002 11:22:34 0200
Date: Fri, 3 May 2002 02:30:55 -0700
From: "Rashmi Dumas"
X-Priority: 3
To: ygrep@is.mgh.mcgill.ca
Subject: The database that Bill Gates doesnt want you to know about!!!!!
Mime-Version: 1.0
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit
```

On notera plusieurs choses qui confirment l'intérêt limité de certains en-têtes. L'en-tête From: a été falsifié pour ne donner aucune information (il n'y a même pas une adresse) ; l'en-tête To: est lui-même faux également (l'adresse de destination était en fait ygrep@usa.net comme on le comprendra par la suite).

Ces bricolages sont extrêmement faciles, mais là s'arrêtent les informations utiles que nous rêvions de retirer des en-têtes traditionnels. Les lignes Received: vont se révéler plus intéressantes et plus explicites.

Si on commence par le haut de la liste on trouve :

```
Received:  from cmsmail08 [127.0.0.1] by cmsmail08 via mtad
(CM.1201.1.04A) with ESMTP id 888gecJI81094M08; Fri, 03 May 2002
09:34:59 GMT
```

Cette ligne est insérée par le système de courrier électronique local de USA.net (le FAI qui a reçu ce SPAM qui m'était destiné). Elle ne donne pas beaucoup d'informations, en particulier, parce que l'adresse IP 127.0.0.1 est une adresse locale sans intérêt. Mais ce n'est pas grave puisque nous savions déjà où est arrivé le message.

Ensuite, on trouve une autre ligne :

```
Received: from baro.antw.online.be [62.112.0.23] by cmsmail08 via smtad
(CM.1201.1.04); Fri, 03 May 2002 09:34:59 GMT
```

On reconnaît maintenant davantage d'information utiles. Le serveur de courrier électronique de USA.net (qui s'identifie toujours aussi pauvrement) a reconnu l'origine du message. Il arrive d'une machine qui s'est identifiée comme baro.antw.online.be. Le serveur en a profité pour noter l'adresse IP de cette machine (62.112.0.23). Une petite visite à un utilitaire whois me permet de confirmer qu'il s'agit bien d'une machine de online.be, qui s'identifie bien par reverse-DNS comme baro.antw.online.be (il n'y a donc aucune falsification ici). En fait le serveur cmsmail08 a décidé de ne

faire aucun commentaire probablement parce qu'il a bien vu que le nom de la machine et l'adresse IP étaient en coïncidence.

La ligne suivante est également intéressante :

```
Received: from server_pdc.aspaburo.be (gateway.aspaburo.be
[194.88.105.138]) by baro.antw.online.be (8.9.3/8.9.3) with ESMTP id
LAA35553; Fri, 3 May 2002 11:29:50 0200 (CEST)
```

La forme est toujours la même, mais cette fois-ci nous sommes remontés encore un cran en arrière. baro.antw.online.be indique d'où il tient le message. Selon lui il provient d'une machine qui se désigne elle-même comme server_pdc.aspaburo.be, a pour adresse IP 194.88.105.138, mais a pour nom officiel gateway.aspaburo.be (selon le reverse-DNS). Il ne s'agit pas là d'une falsification au sens propre du terme. Il est courant d'avoir plusieurs noms pour une même machine selon les usages qui en sont fait.

Jusque là, tout semble normal. Nous nous rapprochons de l'origine.

```
Message-Id: <200205030929.LAA35553@baro.antw.online.be>
```

Cette nouvelle ligne a très probablement été insérée par baro.antw.online.be lors de sa réception du message pour l'identifier alors qu'il ne disposait pas encore d'un Message-Id:.

La ligne qui suit est beaucoup plus étonnante :

```
Received: from smtp0351.mail.yahoo.com (mail.elsystravel.com
[66.12.138.26]) by server_pdc.aspaburo.be with SMTP (Microsoft
Exchange Internet Mail Service Version 5.5.2650.21) id JHNSAL6F; Fri, 3
May 2002 11:22:34 0200
```

Le serveur server_pdc.aspaburo.be nous affirme maintenant avoir reçu ce message d'une machine qui se « présente » comme smtp0351.mail.yahoo.com, mais qui a pour adresse IP 66.12.138.26 et qui répond en fait au doux nom de mail.elsystravel.com.

En fait, si l'on recherche, smtp0351.mail.yahoo.com n'existe pas (et ne répond à aucune requête). Il n'y a là rien d'étonnant : pourquoi un Fournisseur d'Accés Internet géant comme yahoo.com prendrait la peine de faire transiter ses messages à destination de USA.net (un autre gros FAI) par un minuscule serveur de aspaburo.be ?

Cette ligne est bel et bien soit une fabrication pure et simple, soit la trace d'une tentative de camouflage.

Dans le premier cas (fabrication), le message a été « injecté » par server_pdc.aspaburo.be (qui est l'origine du SPAM) à baro.antw.online.be (qui est la première victime et probablement un open-relay).

Dans le deuxième cas (camouflage), le message a été injecté à server_pdc.aspaburo.be (qui est la première victime, probablement un open-relay). Dans ce cas, server_pdc.aspaburo.be nous désigne le coupable. Je penche personnellement pour cette dernière interprétation.

Tout cela ne nous donne pas forcément le nom et l'adresse du coupable. En effet, il n'est pas très difficile d'utiliser la base de données de whois pour identifier les propriétaires de elsystravel.com (la société Elsy's Travel en Californie). Cela ne nous donne pas l'autorisation de les accuser de SPAM. En l'occurence, il est plus vraisemblable qu'il s'agit d'un hacker (ou d'un spammeur un peu mieux outillé que la moyenne) qui a utilisé leurs machines pour envoyer son message. Elsy's Travel est alors la première véritable victime[37].

37 Ne les ennuyez pas ; ils sont effectivement victimes comme nous le verrons plus bas

J'espère que ce parcours à travers un cas simple vous aura donné une meilleure idée de ce qui peut être fait pour comprendre l'origine d'un message de courrier électronique. J'espère également que vous aurez retenu la leçon importante qui est de toujours contrôler tous les détails disponibles jusqu'à obtenir des certitudes (ce n'est pas toujours facile !).

Et n'oubliez pas que le téléphone ou le mail direct à quelqu'un peut vous permettre d'avoir des explications. Le plus souvent vous tomberez sur quelqu'un qui n'est pas au courant du problème, parfois sur quelqu'un de désagréable mais pas un spammeur pour autant, plus rarement sur un spammeur qui essayera de vous faire avaler des couleuvres longues comme le bras.

Ne vous arrêtez donc pas à vos premières impressions et confirmez, vérifiez, puis recommencez.

Dans le cas présent, je peux facilement confirmer la situation par le fait d'avoir reçu plusieurs SPAMs de la même origine. Ils sont tous passés par des chemins différents (y compris la Corée), ils commencent tous par une ligne Received: similaire à celle étudiée ici (le nom inventé du faux serveur yahoo.com change un peu à chaque fois). La vérification est donc venue par encore un autre biais (la confrontation de plusieurs SPAMs de la même origine).

Dans le cas présent, je conseillerais de contacter postmaster@elsystravel.com (ou elsystravel.com@abuse.net) pour lui signaler le problème. Soyez aimable et patient. Dans le feu de l'action, cette personne (s'il y a vraiment une personne en charge de la sécurité informatique d'une société vraisemblablement petite) est probablement surchargée de travail en temps normal et totalement débordée par les problèmes liés à ce viol de relais. Il n'est pas anormal de ne recevoir aucune réponse, il n'est pas anormal de recevoir un mail furieux, énervé ou laconique. Soyez patient et compréhensif.

J'enverrais également un message à postmaster@aspaburo.be (ou gateway.aspaburo.be@abuse.net) pour les aider à gérer le problème également (avec les mêmes commentaires).

Une remarque à propos des adresses IP invalides : dans un certain nombre de cas, l'adresse IP que vous allez trouver dans les en-têtes peut être invalide sans que cela ne soit anormal. N'oubliez pas que les adresses IP sont souvent allouées de manière dynamique (par exemple, chaque fois que vous vous connectez avec un modem à votre FAI, vous obtenez une adresse différente). Il est alors parfois utile de remonter d'un cran en amont en utilisant un utilitaire de type traceroute quivous indiquera surement qui est le fournisseur d'accès de l'utilisateur en question.

7. Internet par e-mail

Ce n'est plus nécessairement la priorité dans notre période d'Internet présent partout (ou presque), mais il y des cas où le courrier électronique est le seul moyen d'accès à Internet qui reste disponible. Il est intéressant de noter l'existence de services qui permettent l'accès (indirect) à la quasi-totalité des services Internet.

Par exemple, il est possible d'accéder à des serveurs FTP ou HTTP avec uniquement un compte de courrier électronique. Il suffit de savoir où envoyer ses requêtes et comment les formuler.

La plupart des informations disponibles ici proviennent de l'excellente FAQ « Internet by email » publiée depuis 1994 par Bob Rankin puis Gerald E. Boyd. La manière la plus simple d'obtenir cette FAQ (en anglais uniquement) consiste à envoyer un courrier électronique à l'adresse mail-server@RTFM.mit.edu en y incluant la ligne suivante :

```
send usenet/news.answers/internet-services/access-via-email
```

Ou bien par le web à l'adresse suivante :

http://www.faqs.org/faqs/internet-services/access-via-email/

On trouvera également une traduction en français par Claude Bay, sur le web à l'adresse suivante :

http://rtsq.grics.qc.ca/saqca/docs/pedagogie/accmail.htm

7.1. FTP par courrier électronique

Enovyer un courrier électronique à l'un des serveurs suivants :

ftpmail@academ.com (Etats-Unis)
ftpmail@btoy1.rochester.ny.us (Etats-Unis)
ftpmail@cnd.caravan.ru (Russie) – Trés lent
ftpmail@dna.affrc.go.jp (Japon)
ftpmail@ftp.sunet.se (Suède)
ftpmail@ftp.uni-stuttgart.de (Allemagne)
ftpmail@gu.net (Ukraine)
ftpmail@ml.imasy.or.jp (Japon)
ftpmail@mail.iif.hu (Hongrie)
ftpmail@mercure.umh.ac.be (Belgique)
ftpmail@uar.net (Ukraine)

Le contenu du (premier) courrier électronique sera soit (pour obtenir un message d'assistance ou un manuel d'utilisation du service) :

```
help
```

soit (pour obtenir la liste du répertoire de tête d'un site FTP) :

```
open <site>
dir
quit
```


En général, les commandes utilisables sont :

Commande	*Rôle*
binary	La commande qui permet de forcer le mode binaire de FTP pour les fichiers qui ne sont pas seulement du texte
cd	Changement de répertoire
chdir	Changement de répertoire
get <file>	Téléchargement d'un fichier

7.2. Que s'est-il passé aujourd'hui ?

Un service tout simple qui permet d'avoir quelques événements en relation avec une date. Envoyer une courrier qui contient simplement « get today today.MMDD » (où MMDD est quelque chose du genre 0317, un mois et une année) in a message to majordomo@angus.mystery.com.

7.3. Autres services par courrier électronique

On peut également rencontrer le même genre de solution pour les services suivants :

- Archie par courrier électronique
- FTP search par courrier électronique
- Gopher par courrier électronique
- Veronica par courrier électronique
- Jughead par courrier électronique
- Usenet par courrier électronique
- World Wide Web (WWW) par courrier électronique
- WWW search par courrier électronique
- Finger par courrier électronique
- WhoIs par courrier électronique

Pour plus de détails, on se reportera à la FAQ anglophone indiquée au début de ce chapitre.

On peut aussi trouver des moyens d'envoyer des fax par l'intermédiaire du courrier électronique. Toutefois, les nombreuses limitations[38] imposent de ne faire que citer cette possibilité.

38 Très petit nombre de destinations possibles (certaines zones géographiques), nombre de pages limité, présentation/forme très contrainte, apparition d'informations spécifiques au service intermédiaire (et qui peuvent provoquer des confusions graves), etc.

8. SPAM et législation

8.1. Préambule

Que les choses soient bien claires dès le début de ce chapitre : je ne suis pas un avocat et on peut certainement trouver des erreurs dans ce qui apparaît plus bas (comme dans le reste de l'encyclopédie). Demandez donc toujours l'avis d'un spécialiste avant de vous engager sur la foi de ce que j'écris ici.

Toutefois, les pages suivantes vont essayer de résumer quelques connaissances dont je dispose sur le sujet. Il s'agit d'un sujet qui est susceptible d'évoluer, mais certains éléments historiques seront utiles.

Pour plus de détails, je vous conseille le site web (en anglais) :

http://www.spamlaws.com/

Vous y trouverez les originaux de certains textes significatifs.

Par ailleurs, vous entendrez sans doute des gens dire que la solution au problème du SPAM passe (ou ne passe pas) par la législation. Même si nous pouvons tous comprendre que les arguments avancés dans une conversation ont parfois besoin d'être simplifiés pour être mieux compris, je crois que dans le cas du SPAM, la simplification n'est pas bonne.

La solution au problème du SPAM passe par un ensemble complet de mesures et de progrès :

- Une législation anti-SPAM
- Des mesures techniques de défense prises par la grande majorité des intervenants
- Une meilleure connaissance et compréhension par le grand public

Aucune de ces choses prises isolément n'apportera de solution. Il les faudra toutes pour revenir à une situation raisonnable.

8.2. Législation américaine

Législation fédérale

Les messages de SPAM contiennent souvent des textes comme :

> This message complies with the proposed United States Federal requirements for commercial e-mail. For additional information see: http://www.senate.gov/~murkowski/commerciale-mail/e-mailAmendText.html. Current information on the status, text, and summary of Title 3 of S. 1618 and H.R. 3888, its companion bill, can be found by using Thomas, the legislative information system run by the Library of Congress.

Ou :

This message complies with the proposed United States Federal requirements for commercial e-mail bill, Section 301. Per Section 301, Paragraph (a)(2)(C) of S.1618, further transmissions to you by the sender of this e-mail may be stopped at no cost to you by sending a reply to this e-mail address with the word "remove" in the subject line. For additional info, see: http://www.senate.gov/~murkowski/commerciale-mail/e-mailAmendText.html.

Malgré l'apparent sérieux de ces déclarations, et les références intimidantes à des textes de loi, la proposition S.1618 du Sénateur Murkowski (qui, pour faire court, proposait de légaliser le SPAM sous certaines conditions légères) a été abandonné en comité avant d'être présenté à la Chambre des Représentants et n'est donc jamais devenu une loi.

http://thomas.loc.gov/cgi-bin/query/z?c105:S.1618:

En conséquence, la simple présence de portions significatives des deux textes précédents dans un courrier électronique constitue pratiquement une signature de spammeur[39] (donc utile pour organiser un filtrage).

D'après EPIC (http://www.epic.org/privacy/junk_mail/spam/), trois propositions de loi (*bill*) ont été présentées à la 104e session du Congrés en vue de résoudre les problèmes posées par le SPAM. Elles proviennent du représentant du New Jersey, Chris Smith (R) et du sénateur de l'Arkansas Frank Murkowski (R) (le 21 mai 1997) et du sénateur du New Jersey Robert Toricelli (D) (le 11 juin 1997). En 1998, le sénateur John McCain a présenté une quatrième proposition de loi.

Netizen Protection Act of 1997 (H. R. 1748)

http://thomas.loc.gov/cgi-bin/query/z?c105:H.R.1748:

Unsolicited Commercial Electronic Mail Choice Act of 1997 (S.771)

http://thomas.loc.gov/cgi-bin/query/z?c105:S.771:

Electronic Mailbox Protection Act of 1997 (S. 875)

http://thomas.loc.gov/cgi-bin/query/z?c105:S.875:

Anti-slamming Amendments Act of 1998 (S.1618)

http://thomas.loc.gov/cgi-bin/query/z?c105:S.1618:

Aucune de ces propositions n'a abouti. Mais le sénateur Murkowski s'est acquis une solide réputation avec sa tentative qui était particulièrement favorable aux spammeurs (elle n'imposait que de marquer « advertisment » dans l'objet du courrier électronique pour que celui-ci devienne légal).

Il faudrait aussi compter quelques autres tentatives comme celle de Bill Tauzin.

Législation d'état

Mais, il existe toutefois des législations à l'intérieur de certains états américains. Elles sont parfois très strictes avec les spammeurs (au point que certains se sont lancé dans la collecte active des dommages et réparations prévus par la Loi).

39 La seule exception à laquelle je pense est que la communauté anti-SPAM peut avoir à parler (par e-mail) de ces propositions de loi dans des courriers électroniques. Soyez donc très attentifs si vous mettez en place un filtrage anti-SPAM qui repose sur cela chez un Fournisseur d'Accès Internet. Mais c'est utile à savoir. Je l'utilise moi-même avec un taux de succès proprement ahurissant.

Gagner de l'argent avec un spammeur

Aux Etats-Unis, c'est devenu une pratique possible, même pour les individus. Les histoires de succès de ce type se retrouvent sur le site anglo-saxon de SpamCon.Org (http://law.spamcon.org/) dans la rubrique « articles ».

8.3. Législation européenne

Au début de l'année 2002, les débats au Parlement Européen ont mené à un vote particulièrement important (30 mai 2002) puisqu'il revient à interdire purement et simplement le SPAM commercial de la part des sociétés européennes. La Directive Européenne qui entrera en application courant 2003 (Ah ! Les lenteurs administratives !) devra préciser que l'envoi de courrier électronique à caractère commercial devra passer par une autorisation préalable (« opt-in »).

Il n'est pas encore clair pour moi si cette Directive pourra être utilisée par un hébergeur dont les abonnés sont victimes d'un SPAM ou si les actions en justice devront être individuelles.

Il également probable que cela n'arrêtera pas le SPAM. Mais si plusieurs grands pays s'engagent dans la voie d'une telle législation, il pourrait devenir possible d'éliminer le SPAM provenant des opportunistes les plus petits et des entreprises.

Le point sur le spamming – par Me Murielle Cahen

Très gentiment, Me Murielle Cahen (une des rares avocats à traiter spécifiquement les problèmes liés à Internet) m'a autorisé à reproduire un article publié sur son site web (www.murielle-cahen.com).

L'original a paru sur http://www.murielle-cahen.com/p_spamming.asp où vous pouvez le retrouver au milieu d'autres articles juridiques tout-à-fait intéressants concernant le droit et Internet.

Bien entendu, l'information présentée ici est susceptible d'évoluer avec le temps (l'original a paru en mai 2002).

Définition et position du problème

Défini par la CNIL comme « l'envoi massif – et parfois répété- de courriers électroniques non sollicités, le plus souvent à caractère commercial, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique dans les espaces publics de l'Internet : forums de discussion, listes de diffusion, annuaires, sites Web, etc. », le spamming, ou « pollupostage », constitue une dérive du marketing en ligne qui permet aux entreprises de « toucher » rapidement, directement et massivement les internautes par le biais de leur boite aux lettres électronique, et de réduire ainsi considérablement l'ensemble des frais qu'il leur faut engager.

Cependant, utilisée massivement depuis 1997, une telle pratique suppose que les entreprises aient préalablement collectées les adresses, auxquelles elles envoient ces courriers non sollicités, conformément aux dispositions des législations de protection des données (loi « Informatique et liberté » du 6 janvier 1978, directives européennes du 25 octobre 1995, du 20 mai 1997 et du 15 décembre 1997).

En effet, l'adresse électronique constitue une donnée personnelle au sens de ces législations. Or, bien souvent, cette collecte se fait de façon sauvage au moyen de « logiciels aspirateurs » d'adresses présentes sur les listes de diffusion ou les forums de discussion.

De plus, il est possible de se procurer, sur Internet et pour une somme dérisoire, des CD-ROM contenant jusqu'à 60 millions d'adresses.

La pratique du spamming pose donc deux problèmes au regard des règles relatives à la protection des données personnelles que constituent les adresses e-mail :

- celui des conditions de collecte et d'utilisation de ces données personnelles à des fins de prospection, notamment quand cette collecte a lieu dans les espaces publics de l'Internet
- celui de l'appréciation des moyens mis en œuvre pour permettre aux personnes prospectées de s'y opposer (« opt-in » et « opt-out »)

Typologie et conséquences du spamming

Le spamming est susceptible d'affecter trois types de ressources Internet : les forums de discussion, les moteurs de recherche et le courrier électronique.

Dans le premier cas, il peut consister en des pratiques de multipostage abusif, Excessive Multi-posting (EMP) et Excessive Cross Posting (ECP), qui vont perturber le fonctionnement des forums de discussion.

Ces pratiques peuvent être identifiées et quantifiées à l'aide d'outils spécifiques, outils permettant de prendre la mesure de la nocivité des envois réalisés en nombre sur les groupes de discussion.

Ainsi, l'envoi d'un même message à plusieurs groupes identifiés pendant une période de 45 jours conduit à retenir la qualification de spamming.

Mais précisons que ce seuil n'est qu'indicatif car d'autres paramètres, tels que la méthode employée ou la quantité de messages envoyés, sont également pris en compte.

Dans une seconde hypothèse, le spamming peut correspondre à une indexation abusive dans les moteurs de recherche. On parle alors d'engine spamming ou de spamdexing.

Pour lutter contre une telle menace, les principaux moteurs de recherche ont mis en place de nombreuses solutions techniques.

A titre d'illustration, le moteur de recherche d'Infoseek procède au déclassement automatique de tout site contenant plus de sept mots identiques.

Enfin, le spamming peut se manifester au travers du courrier électronique qui est devenu le principal vecteur commercial des entreprises actives sur le réseau Internet.

La raison tient simplement au fait que contrairement à la prospection traditionnelle (effectuée par voie postale, téléphonique ou par télécopie) qui faisait peser la totalité des frais de prospection sur l'expéditeur, le courrier électronique ne présente qu'un très faible coût.

Ces entreprises recourent à des techniques aussi diverses que les lettres d'information contenant des hyperliens ou que les messages d'alerte.

En matière de courrier électronique, la qualification de spamming dépendra généralement de deux critères :

- le caractère non sollicité du message envoyé (dont l'objet publicitaire le transforme en message promotionnel non sollicité),
- les charges que ces courriers génèrent au détriment du destinataire et du fournisseur d'accès (« cost-shifting »).

Ces spams vont avoir pour conséquences d'engorger le réseau, d'augmenter les délais de connexion lors de la réception des messages et donc les frais supportés par les fournisseurs d'accès forcés de mettre en place un filtrage adapté.

Ceux-ci se retrouvent dans l'obligation de répercuter les coûts sur les offres d'abonnement.

Ainsi, selon une étude commandée par la Commission européenne, les abonnés à l'Internet paieraient, à leur insu, un montant estimé à 10 milliards d'euros par an en frais de connexion, cela uniquement pour recevoir des messages non sollicités.

On comprend donc la nécessité d'une réglementation efficace du spamming.

Le publipostage électronique peut s'effectuer à l'égard de clients ou de visiteurs d'un site web, à l'égard de prospects grâce à des listes d'e-mails fournies par un tiers ou collectées dans les espaces publics de l'Internet.

Seule cette dernière hypothèse pose réellement problème.

Dans le premier cas, la collecte est directe puisque le fichier d'adresse est constitué à partir des mails des internautes avec lesquels le prospecteur s'est trouvé en contact direct. Les règles de protection des données personnelles autorisent alors l'envoi de courriers électroniques de prospection à condition de respecter le droit de chaque internaute de s'opposer à en recevoir ; ceci suppose qu'il ait été informé et mis en mesure d'exercer son droit d'opposition lors de la collecte initiale de ses données personnelles.

Dans le cas où le publipostage se fait à partir de listes d'adresses fournies par un tiers, la collecte est indirecte. L'internaute a communiqué son e-mail à un site qui a ensuite cédé son fichier de mails à un tiers aux fins de prospection.

Là encore, si l'internaute a été informé lors de la collecte initiale de ses données personnelles de cette possibilité et qu'il a été mis en mesure de s'y opposer, alors la collecte sera considérée comme licite.

La dernière hypothèse suppose que l'e-mail de l'internaute ait été capturée dans un espace public (forums de discussion, listes de diffusion…) sans que celui-ci ou le responsable de l'espace diffusant les données n'en ait eu connaissance. Cette collecte déloyale rendrait illicite toute les opérations de traitement ultérieures.

Précisons que la réglementation du spamming est envisagée à travers « l'opt-in » (opter pour) et « l'opt-out » (opter contre).

L'opt-in oblige les prospecteurs à obtenir le consentement des internautes à recevoir des sollicitations préalablement à tout envoi de courrier électronique.

Quant à « l'opt-out », elle est plus avantageuse pour les prospecteurs car ils peuvent directement démarcher les internautes qui ne peuvent s'opposer à l'envoi de sollicitations qu' a posteriori.

Rappelons les principales législations adoptées en Europe et aux Etats-Unis ainsi que les droits qu'elles accordent aux internautes et obligations qu'elles mettent à la charge des prospecteurs.

La réglementation : état des lieux et perspectives

Depuis 1997 la réflexion juridique relative au spamming a beaucoup évolué.

La directive CE du 24 octobre 1995 relative à la protection des données personnelles ne traite pas spécifiquement de la prospection électronique, mais elle s'applique toutefois aux traitements des données personnelles mis en œuvre sur Internet.

Elle reprend en partie le contenu de la loi de janvier 1978 et pose plusieurs principes relatifs à la finalité et à la loyauté de la collecte, à la légitimité du traitement, à l'information des personnes ainsi qu'au droit d'opposition dont elles bénéficient.

Ainsi, son article 6.1(a et b) prévoit que « les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités », c'est à dire de façon loyale et licite.

Son article 7 précise qu'un traitement de données ne peut être légitime qu'à la double condition d'être nécessaire au but légitime poursuivi par son responsable et que la personne concernée ait « indubitablement » donnée son consentement. Ces deux conditions sont appliquées en matière de prospection électronique.

La nature de l'information délivrée aux personnes dans les hypothèses de collecte directe ou indirecte et les droits attachés à chaque type de collecte sont rappelés : finalité et caractère facultatif ou obligatoire de la collecte, destinataires des données collectées, existence d'un droit d'accès et de rectification, existence d'un droit gratuit et sur demande de s'opposer au traitement de ses données à des fins de prospection, possibilité de refuser toute communication ou utilisation de ses données par des tiers.

La directive du 15 décembre 1997 (article 12) complète le dispositif de la directive de 1995 en imposant un consentement préalable exprès des consommateurs pour l'utilisation d'automates d'appels ou de télécopieurs dans des opérations de prospection directe.

Quant aux opérations de prospections autres que celles recourant à des automates d'appels, il appartient aux Etats de choisir entre l'exigence d'un consentement préalable et exprès du destinataire (opt-in) ou un droit d'opposition de la part du destinataire, avec possibilité d'une inscription dans un registre spécifique (opt-out).

Lorsque le choix se porte vers « l'opt-out », la directive du 8 juin 2000 impose que des mesures d'accompagnement soient adoptées : identification claire et non équivoque, par l'expéditeur des communications commerciales, de la personne pour le compte de laquelle ces communications sont faites ; identification de la nature commerciale des messages dès leur réception par le destinataire.

La directive européenne du 20 mai 1997, dite « directive vente à distance » et qui devait être transposée avant ?, consacre le système de « l'opt-out » en son article 10 (l'internaute doit choisir de ne pas recevoir de mails), tout en laissant la possibilité aux Etats membres de choisir « l'opt-in ». C'est ainsi que l'Allemagne, l'Italie, la Finlande, l'Autriche et le Danemark ont consacré « l'opt-in » pour réglementer la pratique du spamming sur leur territoire.

La France n'a d'ailleurs transposé partiellement cette directive que par une ordonnance du 23 août 2001.

Son article 12 introduit un nouvel article L. 121-20-5 du Code de la consommation et consacre le système de « l'opt-out » pour la prospection commerciale par courrier électronique non sollicité et dont les modalités d'application seront fixées ultérieurement par un décret pris en Conseil d'Etat.

Cette transposition devance et annule une disposition du projet de loi sur la société de l'information du 18 juin 2001(article 22) qui consacrait « l'opt-out » en insérant un nouvel article au Code de la consommation (L. 121-15-1) tout en prévoyant des mesures d'accompagnement.

Cet article 22, reprenant l'article 7 de la directive du 8 juin 2000, exige une identification claire et non équivoque des publicités non sollicitées et des offres promotionnelles adressées par courrier électronique, et cela dès leur réception par leur destinataire.

De plus, sur chaque message non sollicité, une mention doit apparaître et indiquer au destinataire qu'il existe des registres d'opposition lui permettant d'exercer son droit de refuser ces envois.

Enfin, le projet de LSI précise expressément que ces nouvelles dispositions s'appliquent également aux e-mails non sollicités à destination des professionnels.

Le 13 novembre 2001, le Parlement européen adoptait une proposition de directive « concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques » ; il y consacrait le système de « l'opt-in » dans son article 13 mais uniquement pour les SMS, se prononçait contre l'emploi des cookies sans le consentement de l'internaute, mais laissait le choix aux Etats quant au système à adopter en matière d'e-mails non sollicités.

Suite à cette proposition, un rapport était rendu mais optait pour le système de « l'opt-out » par peur que le système de « l'opt-in » ne constitue une entrave au développement du commerce électronique en Europe par rapport aux autres régions du monde.

Le Conseil européen, suite aux vives critiques suscitées par la position du Parlement, a finalement adopté une position commune sur cette directive le 21 janvier 2002 et a pris position en faveur de « l'opt-in », les Ministres européens des télécommunications s'étant par ailleurs clairement prononcés pour « l'opt-in » le 6 décembre 2001.

Les Etats membres n'ont donc plus le choix entre les deux systèmes.

Selon son article 13 « l'utilisation de (…) courrier électronique à des fins de prospection directe ne peut être autorisée que si elle vise des abonnés ayant donné leur consentement préalable ».

Dès lors que l'adresse de l'émetteur n'est pas clairement précisée ou s'il s'agit d'une fausse adresse, toute communication de cette nature sera formellement prohibée.

Quant aux Etats, ils doivent veiller à ce que les personnes morales soient suffisamment protégées en ce qui concernent les communications non sollicitées.

Néanmoins, le texte prévoit que lorsque les coordonnées électroniques d'un client sont obtenues directement, c'est à dire dans le respect de la directive de 1995, par une personne dans le cadre d'un achat d'un produit ou d'un service, ladite personne peut exploiter ces coordonnées à des fins de prospection directe pour des services ou produits analogues.

Mais il existe une condition : les clients doivent avoir la faculté de s'opposer, sans frais et de manière simple, à une telle exploitation lors de leur collecte ou de chaque message.

Ce texte est le premier à différencier le régime applicable à l'utilisation du courrier électronique à des fins de prospection directe selon que les adresses ont été obtenues directement ou non par l'expéditeur des messages.

Le Parlement européen a réaffirmé le principe de l'opt-in pour l'envoi de « communications non sollicitées effectuées à des fins de prospection directe ».

Le texte doit ensuite passer devant le Conseil des ministres pour être définitivement approuvé puis, il sera publié au Journal Officiel vers fin juillet 2002. Les Etats membres disposeront alors d'un délai de 15 mois pour transposer la directive dans leur législation nationale.

Quant aux Etats-Unis, la situation n'est guère différente. Trois Etats américains (Washington loi du 25/03/1998 ; Californie li du 26/09/1998 et Névada en 1999) prohibent et sanctionnent d'une lourde peine d'amende l'envoi de courriers électroniques à caractère commercial non sollicités par leurs destinataires.

Outre le Telephone Consumer Protection Act (1991) qui prohibe la prospection non sollicitée par voie de télécopie et que certains souhaitent voir étendu aux courriers électroniques, il nous faut évoquer le Unsolicited commercial Eletronic Mail Act of 2000 (17 juin 2000) qui retient le système de « l'opt-out ».

Notons qu'un projet de loi visant à lutter contre l'envoi de courriers non sollicités sera soumis au vote du Comité du Sénat en charge du Commerce le 16 mai 2002 ; Ce projet prévoit l'obligation pour les entreprises de e-marketing de faire figurer sur ces courriers une adresse e-mail valide, afin de permettre à leurs destinataires de proscrire le cas échéant ce type de messages, et ce sous peine de sanctions pénales.

De même, le projet se prononce en faveur de la prohibition de la pratique qui consiste à faire figurer des titres à caractère trompeur, et sans relation avec le contenu du message, afin d'inciter le destinataire à en prendre connaissance.

Il prévoit également le renforcement des pouvoirs de la Federal Trade Commission (FTC) : elle pourra infliger aux entreprises fautives des amendes pouvant aller jusqu'à $30 par e-mail envoyé, et au maximum de $1 500 000.

Quant aux Procureurs, ils pourront engager des poursuites judiciaires contre ces entreprises.

La législation américaine a décidé d'imposer une amende de 10 $US par pourriel, avec un plafond de 500 000 $US. Une proposition de loi a été votée en mai 2002 par le Sénat américain, et approuvée unanimement par les Démocrates et les Républicains.

Jurisprudence récente

France

Pour la première fois en droit français la pratique du spam a été condamnée par une ordonnance de référé du TGI de Paris (15 janvier 2002).

Le juge Jean-Jacques Gomez (affaires « Yahoo » et « J'accuse ») a estimé cette pratique « déloyale et gravement perturbatrice » et contrevenant ainsi au contrat passé entre l'auteur du spam et son fournisseur d'accès à internet.

En l'espèce, l'internaute spammeur avait engagé une action contre ses FAI (Free et Liberty-Surf) pour rupture unilatérale de contrat, ces derniers ayant coupé ses accès Internet devant l'importance des spams constatés. L'internaute a donc été condamné à payer la somme de 1524 euros à ses FAI pour procédure abusive.

Cette décision semble s'inscrire dans le cadre de plusieurs directives européennes qui devraient interdire ce type de pratique.

Une affaire dont les faits sont similaires avait déjà été jugée par le TGI de Rochefort sur Mer le 28 février 2001.

En l'espèce, un internaute intentait une action contre son FAI pour rupture unilatérale de son contrat.

Cette rupture faisait suite à la constatation d'un envoi massif de messages publicitaires en direction des forums de discussion, par cet internaute, et dans le but de développer ses activités commerciales; cet envoi fut d'ailleurs dénoncé par de nombreux utilisateurs.

Sommé de respecter les usages en vigueur et de stopper cette pratique sous peine de voir son contrat interrompu « immédiatement et sans préavis », l'internaute a pourtant persisté, pensant que le spamming à l'encontre des forums de discussion n'était pas prohibé.

Le tribunal va pourtant débouter le demandeur au motif que l'usage constitue une source de droit et qu'à ce titre il « s'impose à celui qui se livre à une activité entrant dans son champ d'application » ; c'est donc à bon droit que le FAI pouvait résilier de façon unilatérale le contrat le liant à son abonné.

Les juges visent l'article l'article 1135 du Code Civil qui prévoit que « les conventions obligent non seulement à ce qui y est exprimé, mais encore à toutes les suites que l'équité, l'usage ou la loi donnent à l'obligation d'après sa nature ».

Notons que contrairement au TGI de Paris, l'internaute n'avait pas été condamné pour procédure abusive par le TGI de Rochefort sur Mer.

Etats-Unis et Canada

La Cour supérieure de l'Ontario s'est pour la première fois prononcée sur une affaire traitant du spamming en 1999 (Cour supérieure de l'Ontario, aff. 1267632 Ontario Inc. c. Nexx Online Inc, 09/07/1999).

Dans ce cas, un prestataire de services canadien (Nexx Online) prend la décision de fermer le compte d'hébergement d'une société cliente (Ontario, Inc.) gérant un site, au motif que ce site avait procédé à un envoi massif de courriers non sollicités (plus de 200 000 par jour) grâce aux service d'un autre prestataire.

Or, le contrat d'hébergement les liant renvoyait expressément aux règles de la « Netiquette » qui prohibe une telle pratique.

La société Ontario Inc décide donc de poursuivre son prestataire Nexx Online pour non respect de ses obligations contractuelles. Analysant les termes dudit contrat, le juge constate qu'aucune clause apparente n'interdisait au client de distribuer des courriers commerciaux non sollicités.

Cependant, la Cour relève l'existence de deux clauses par lesquelles le client s'engage par l'une, à respecter la « Netiquette », et par l'autre à accepter l'adjonction de nouvelles conditions contractuelles. Or, le prestataire de services avait informé son client, quelques mois avant la constatation de la pratique interdite, qu'il n'accepterait aucune distribution de courriers commerciaux non-sollicités à l'aide de ses services.

La « Netiquette » constitue un ensemble de règles de savoir vivre que se doivent de respecter les utilisateurs d'Internet, à savoir « un code en évolution, non écrit et basé sur les principes de bon voisinage pour un développement ordonné de l'Inforoute ».

Cette affaire a permis au juge, malgré l'absence de jurisprudence canadienne, de conférer une force juridique aux règles non-écrites de la « Netiquette » en matière de spamming en les déduisant d'un ensemble de documents, dont l'article d'un auteur américain, mais surtout de principes résultant de la jurisprudence dégagée par les tribunaux aux Etats-Unis.

Selon cette jurisprudence, l'envoi de courriers non sollicités en grand nombre s'avère contraire aux principes de la « Netiquette », sauf si le fournisseur de services prévoit, par contrat, un tel envoi.

Précisons que 18 états ont dores et déjà adopté une législation visant à lutter contre le spamming, la Californie condamnant même les auteurs de spams à une amende de 58 euros par message non sollicité envoyé.

La Cour Suprême californienne a d'ailleurs récemment confirmé que la loi anti-spam en viguer dans cet Etat ne contrevient pas à la Constitution américaine (avril 2002).

Quant à la juridiction canadienne, elle a conclu sur le fait que « la pratique du spamming, au mépris de la déontologie en vigueur sur le Réseau, a justifié la déconnexion du site ».

Précisons qu'en application de l'article 1434 du code civil québecois, la « Netiquette » pourrait s'imposer aux parties contractantes même en l'absence de clauses y faisant expressément référence.

Me Murielle Cahen
(avec son aimable autorisation)
www.murielle-cahen.com

9. Programmation

9.1. Expressions régulières utiles

Le RFC 822 décrit formellement la syntaxe à respecter pour décrire une adresse de courrier électronique, mais la plupart des programmeurs ont du mal à rédiger un code capable de vérifier la conformité d'une adresse donnée (par exemple, pour s'assurer qu'une adresse fournie dans un dormulaire est effectivement valide). Cela provient essentiellement de l'extrême complexité de cette syntaxe.

Toutefois, afin de rendre service à ceux qui en auraient besoin, je vous propose une expression régulière qui assure cela dans une majorité des cas. Elle peut être utilisée pour valider les adresses en limitant fortement les adresses improbables tout en ne produisant pas de faux négatifs (cas où l'adresse serait refusée comme non conforme alors qu'elle est conforme).

```
^ [ ^ @ ] + @([a-z0-9.\_\-] + \.) + ([a-z0-9\-]{2} | arpa | net | com | gov | mil | org | edu | int | info | name | biz | aero | coop | museum | pro)$
```

Cette expression est le fruit d'une expression écrite par Manuel Lemos, puis révisée par Christian Lescuyer, et enfin d'améliorations que j'ai personnellement apportées. Elle est utilisée quotidiennement sur des sites web qui ont permis de confirmer son exactitude. Il s'agit d'une approximation (un compromis relativement efficace entre l'exactitude absolue et une calculabilité raisonnable).

```
^ [a-z0-9\._-] + @([a-z][a-z0-9-]{1,62})(\.[a-z][a-z0-9-]{1,62}) + $
```

est une autre expression régulière (qui n'a pas encore été testée en vraie grandeur). Elle a l'avantage de limiter la taille des champs de l'adresse. Je vous conseille de ne l'utiliser qu'après contrôle et test élaborés (que je compte faire également). Et probablement, dans le futur, je combinerai les meilleurs attributs de ces deux expressions régulières.

Remarque importante : ces deux expressions s'appliquent à des adresses qui sont écrite en lettres minuscules (sans majuscules). Il convient donc de commencer par forcer la présentation en minuscules par un appel à une routine comme maj2min(), tolower(), ou tout autre équivalent dans le langage de programmation utilisé.

9.2. Quelques libraries utiles

Nom	*Langage*	*Commentaires*
HTML MIME mail	Classe PHP	http://www.phpguru.org/
LibMail v1.3	Classe PHP	Auteur : Leo West Documentation en français. GPL (gratuit). http://lwest.free.fr/doc/php/lib/index.php3?page=mail&lang=en
CSMTPConnection	C++ (une classe MFC)	Auteur : PJ Naughter Freeware. http://www.codeproject.com/internet/csmtpconn.asp
Perl SendMail Module	PERL	http://www.tneoh.zoneit.com/perl/SendMail/
Perl Mail::Sender	PERL	Auteur : Jan Krynicky http://jenda.krynicky.cz/
vbSendMail	Visual Basic	
librfc822 (RFC822 address parser library 1.0)	C	Auteur : Peter Simons Freeware. Librairie écrite en C qui se veut absolument complète en ce qui concerne la reconnaissance de la validité d'une adresse (ce qui reste inhabituel dans ce domaine). http://www.cryp.to/librfc822/

9.3. Quelques programmes utiles

Je signale au passage quelques programmes qui peuvent être utiles dans la gestion du courrier électronique ou la lutte contre le SPAM.

Nom	*Langage*	*Remarques*
nospam_php	Programme en PHP	http://www.hotscripts.com/Detailed/15064.html Auteur : Martin Bolduc Freeware qui utilise une liste noire provenant du site SpamAnti.net.

9.4. Code de loopback

Pour réaliser une adresse de loopback (celle qui a servi à la création de ce script n'est malheureusement plus accessible[40]), J. Daniel Smith de bristol.com a écrit le code suivant :

```
#
# J. Daniel Smith
# 1 May 1996
#
# loopback.rc - bounce a message back to the sender
#

#####
##### Initial setup needed for *all* procmail invokations
#####
PATH=/bin:/usr/bin:/usr/ucb:/usr/local/bin
SHELL=/bin/sh

MAILDIR=/tmp

# log everything verbosely, since I want to see how all this works
# this needs to be near the beginning of the file to turn logging on ASAP
#LOGFILE=$MAILDIR/LOG
#VERBOSE=on

# define the local top-level domain and fully-qualified domain names
DOMAIN=bristol.com
FQDN=${DOMAIN}

#####
##### Extract/generate interesting mail headers
#####
# get the date in RFC822 format for insertion into some messages;
# the "Resent-Date:" field is copied from the "Date:" field on some systems.
# RFC1123 says "All mail software SHOULD use 4-digit years in dates..."
# sun4 doesn't recognize all "date" flags
#year=`date '+%y'`
#DATE=`cent=19; if [ $year -lt 70 ]; then cent=20; fi; date "+%a, %d %h $cent%y %T EST"`
DATE=`date '+%a, %d %h %Y %H:%M:%S %Z'`

# prevent mail loops
:0
* ^FROM_DAEMON
/dev/null

# large messages are simply bounced back; 69 = EX_UNAVAILABLE
```

40 Pour voir d'autres adresses de loopback du même type mais encore accessibles, on se reportera utilement à l'article loopback de l'encyclopédie.


```
TRAP="exit 69;"
EXITCODE=69
:0
* > 7000
/dev/null
EXITCODE=0
TRAP=""

HOSTNAME=`hostname`
:0c:
loopback.$$
:a
|(formail -rt \
        -I "Reply-To: Postmaster@$DOMAIN" \
        -I 'Precedence: junk' \
        -I 'MIME-Version: 1.0' \
        -I 'Content-Type: multipart/mixed; boundary="-- next item ----"'; \
  echo "This is the preamble of an RFC-1521 encoded, mixed message."; \
  echo "---- next item ----"; \
  echo "Content-Type: text/plain"; \
  echo "Context-Description: bristol.txt"; \
  echo ""; \
  echo "Your message was received at $DOMAIN on $DATE"; \
  echo "Bristol Technology is the leading supplier of cross-platform"; \
  echo "development solutions, including Wind/U, HyperHelp and XPrinter."; \
  echo "For details, visit our WWW site at http://www.bristol.com"; \
  echo ""; \
  if [ "$HOST" != "" ]; then \
    echo "This machine ($HOST) is located at the Bristol offices:"; \
  else \
    echo "This machine ($HOSTNAME) is located at the Bristol offices:"; \
  fi; \
  echo "41.28N -73.45W; 241 Ethan Allen Hwy, Ridgefield, CT;  +1 203 438 6969"; \
  echo ""; \
  echo "Questions about this message should be sent to postmaster@$DOMAIN"; \
  echo "---- next item ----"; \
  echo "Content-Type: message/rfc822"; \
  echo "Context-Description: bounce.txt"; \
  echo ""; \
  formail -I "From " < $MAILDIR/$LASTFOLDER; \
  echo "---- next item ------"; \
  ) | ($SENDMAIL -t; rm -f $MAILDIR/$LASTFOLDER)

# don't want to save any messages away
:0
/dev/null
```

Je reproduis ici intégralement ce code qui a d'abord été « publié » par l'auteur sur Internet et dans un courrier électronique qui peut être retrouvé sur :

http://www.rosat.mpe-garching.mpg.de/mailing-lists/procmail/1997-02/msg00263.html

Il fait usage de procmail et peut être ré-appliqué dans des conditions proches sur un autre domaine que celui de bristol.com.

10. Index

Chaque nom apparaît suivi d'un (ou plusieurs) numéro(s) de page où les références indiquées se rencontrent dans l'encyclopédie. Quand plusieurs numéros de page sont présents, il y a plusieurs pages à consulter. La mention « sv » après un numéro de page indique que les pages suivantes sont également concernées (par exemple, la mention « 7 sv » doit se comprendre comme « pages 7 et suivantes »).

11. Bibliographie

[1] Jargon File 4.0.0 – Eric Raymond – 24 juillet 1996

[2] Le jargon français – Roland Trique – 14 décembre 2001 (http://www.linux-france.org/prj/jargonf/)

[3] Dicofr.com (le dictionnaire de l'informatique) – Eric Goguey – (http://www.dicofr.com/)

[4] Email Abuse FAQ version 2.02 – WD Baseley – (http://members.aol.com/emailfaq/emailfaq.html et ftp://members.aol.com/emailfaq/emailfaq.txt)

[5] Définitions de l'Internet Mail Consortium – (http://www.imc.org/terms.html)

[6] Listes de logiciels de mail (clients, serveurs, passerelles, services, etc.) – Andrew II – (http://asg.web.cmu.edu/cyrus/email/email.html)

[7] Email references – (http://www.newt.com/email/references.html)[41]

[8] Making DNS easy™ – Men and Mice – (http://www.menandmice.com/index.html)

[9] A beginner's guide to effective e-mail – Kaitlin Duck Sherwood – (http://www.webfoot.com/advice/email.top.html)

[10] Finding Someone's Email Address – Kaitlin Duck Sherwood – (http://www.webfoot.com/advice/FindingEmailAddresses.html)

[11] Urban Legends (http://www.urbanlegends.com/)

[12] Des essais (en anglais) sur le SPAM – Brad Templeton – (http://www.templetons.com/brad/spume/)

[13] Put a Spammer in the Slammer - Phil Agre - Comment arrêter un spammeur (en anglais mais très complet) (http://www.user-groups.net/Library/WEB/spammer/default.html#index)

[14] Les abus du réseau - Eric Demeester - FAQ : comment réagir aux messages abusifs (http://www.teaser.fr/~edemeester/abus.htm)[42]

[15] Virus (définitions, mécanismes et antidotes) – Campus Press

[16] E-mail protection antivirus – First Interactive

On complètera cette liste avec l'excellent moteur de recherche sur Internet, Google (http://www.google.fr/) qui représente à lui tout seul une source inestimable d'informations. Je l'ai abondamment utilisé pour confirmer certaines informations et en trouver d'autres.

41 N'a malheureusement pas été mis à jour depuis 1997...
42 Toujours d'actualité et de qualité, même si elle n'a pas été mise à jour depuis 1997.

