Jean-Michel Yolin **vendredi 31 octobre 2003**

SPAM, nouvelle forme de pollution: une explosion en 2003 avec les virus pilleurs de carnet d'adresse, les robots harvester et le rétrospam. Comment se protéger?

1 Quelques données sur le SPAM

Le SPAM, courrier non sollicité, ou pourriel de nos amis canadiens ou "harrassement textuel" des humoristes montmartrois est devenu un vrai fléau : l'origine du mot se trouve dans un sketch des Monthy Pytons ou cette production charcutière américaine acronyme de ***Spiced Pork And Ham*** envahissait progressivement la scène dans un humour à la finesse toute britannique....

le nombre de messages publicitaires non sollicités s'élevait en 2002 à plus d'un milliard et demi par semaine

Sur 2003 on estime à 100Milliards par JOUR le nombre de SPAM qui ont pollué le réseau

Cette pollution a un cout pour les entreprises et les fournisseurs d'accès : elle représentait selon le commissaire européen Frits Bolkenstein, **10 milliards d'euros par an dans le monde** , chiffre voisin de celui publié par l'institut Ferris Research (10G$). *www.eu-oplysningen.dk/euidag/dagspressen/berlingske/84952* Ce chiffre a du augmenter d'un ordre de grandeur en 2003

D'après certaines études parues durant l'été 2003 le Spam est en train d'exploser *http://www.ftc.gov*, *http://www.technologyreview.com/articles/schwartz0703.asp*: Le pourcentage de courriers électroniques non désirés (spam) est passé de 8% en 2000 à 40% à la fin 2002 aux Etats-Unis et représentait au printemps 2003 la majorité de l'ensemble des e-mails. En suivant cette tendance, ce taux pourrait passer bientôt à 90%, saturant les réseaux et "taxant" le temps de chacun et les finances de ceux qui ne bénéficient pas de tarifs forfaitaires

AOL estime pour sa part que 80% des messages transitant sur son service relèvent du SPAM

De plus, pour mieux attirer le client les messages sont bien souvent agrémentés de photos "de qualité", ce qui augmente considérablement l'encombrement généré sur les réseaux

Là encore les études sus-mentionnées chiffrent maintenant à plusieurs dizaines de milliards de $ le cout de cette pollution pour la collectivité alors que le cout de sa production est quasi nul (0,01$ d'après l'agence eMarketer, à rapprocher au mailing postal ou le télémarketing :1 à 3$)

2 Qui sont les spammeurs? Pourquoi le SPAM? Leurs techniques? Quel "business model"?

En France parmi les émetteurs de Spam il y a bien entendu la PME française qui vient de découvrir Internet et à qui sa "webagency" a vanté les économies postales qu'elle pouvait réaliser

J'ai ainsi reçu d'un vigneron d'Albi, après une conférence que j'y avais faite, son catalogue complet qui "pesait" 3Mo : il avait mis une photo de chacune de ses bouteilles et en clair …. la liste de tous ses clients en copie...

Ces PME prennent en général en retour une volée de bois vert au premier envoi et en général on en reste là

Après un grand battage médiatique la CNIL n'a "épinglé" que 5 entreprises (sans qu'il soit même évident qu'une infraction juridique soit constatée) se ridiculisant un peu sur ce dossier en agissant avec l'efficacité d'une bombe de Begon vert sur les cafards de tout un quartier de New York

Mais le véritable problème n'est évidemment pas là : les SPAM qui nous envahissent viennent du monde entier, le plus souvent en anglais mais parfois en chinois… et sont issus de "spammeurs" professionnels

Les spammeurs, qui partent de fichiers de piètre qualité, ont mis au point un certain nombre de moyens pour les améliorer

- le plus rustique est de vous proposer de vous "désabonner" : si vous le faites vous confirmez votre adresse et le fait que vous avez lu le message
- plus sophistiqué, l'inclusion d'une image de taille nulle qu'un script va automatiquement chercher sur un serveur, en fait ceci a pour seul but de transmettre au susdit serveur l'adresse qui a permis de vous spammer en validant celle-ci et en indiquant que vous avez bien ouvert le message

Un exemple transmis par José Marcio Martins da Cruz de l'Ecole des Mines : extrait du script :
<IMG src="http://votech.net/rc/imge.asp?test=Jose-Marcio.Martin@ensmp.fr" height=0 width=0 border=0>
ce javascript va "charger une image" sur le serveur "votec.net", en fait cette opération a pour seul objectif de valider votre adresse qu'il transmet dans cette fausse requête

- Enfin, un lien actif programmé pour transmettre quand vous cliquez dessus l'adresse qui a permis de vous joindre, ajoutant une information : vous êtes curieux!

Exemple d'un lien contenu dans un SPAM récent : il transmet sans doute, outre mon adresse, les coordonnées de celui à qui il faut verser une commission pour m'avoir incité efficacement à aller sur le site : http://t1.2asdf894sadf3sd748dsf9sd2f3744asdfsakdfj928458727a234asdf824aa4aaz.vg/track4.php/FBF482F0049/fast/1?__email=yollin%40yollin.net

Quand vous êtes victime de tels envois, **ne cédez pas à la tentation de répondre** à l'invitation "si vous souhaitez ne plus recevoir d'information de notre part, renvoyez-nous ce mail", bien souvent vous ne faites alors

que valider votre adresse ce qui en accroît la valeur…surtout si dans votre signature ou dans votre "carte" figurent vos coordonnées, de même, bien souvent le simple fait de l'ouvrir provoque une requête vers un serveur transmettant l'adresse

A l'évidence il y a derrière ce phénomène un **modèle économique** extrêmement sophistiqué et parfaitement bien organisé qui explique le développement exubérant d'une telle activité: Il ne nous a pas encore été possible à cette date d'en démonter totalement le mécanisme

Ceux qui vous apparaissent, les "**fantassins**" du spam, sont semble-t-il souvent des personnes qui ont besoin d'arrondir leurs fins de mois : une étude avait été faite par BNP-Paribas en son temps, sur l'industrie du porno qui montrait que le profil type de ces spammeurs-webmestres correspond à des "ménagères de moins de 50 ans souvent seules avec des enfants et peu de ressources"

Il y aurait une formation qui leur serait assurée par une Ecole à Chicago qui connaîtrait un grand succès. Il est vraisemblable qu'ils y sont dotés du "kit" du spammeur (bases d'adresses, maquettes de sites (templates), système de brouillage de piste pour les envois,……)

Leur rôle serait simplement d'appâter le client et de le rabattre vers des sites gérés par de gros professionnels qui eux ne se mettent jamais en infraction et sont à la tête d'un énorme business sans doute très profitable. Ces rabatteurs seraient payés à la commission en fonction des clients captés

Il semble donc s'agir d'une organisation type "tupperware" et il est vraisemblable qu'il en va de même dans les grands créneaux du SPAM : arnaque nigériane, v1agra, développeurs de masculinité, rajeunisseur, prets hypothécaires à bas taux, vendeurs de drogue,...

Les **professionnels qui sont derrière** ont toujours été à la pointe de la technologie et ce sont eux qui ont inventé bon nombre des technologies des web commerciaux (pop-up, pop down, moyens de paiement sécurisés qui ne laissent pas de trace, mouse trapping, utilisation de la large bande pour les flux vidéo,...).

Ils agissent aussi sans vergogne avec des **techniques de pirates** : par exemple ils ont très tôt utilisé la fonction "relais" des serveurs pour effectuer leurs envois de masse (en 2003 ce sont les serveurs chinois et coréens, moins bien protégés qui ont été les principales victimes, subissant ainsi d'un coté les coûts d'expédition et d'un autre une paralysie car ils se trouvaient placés sur des listes noires (blacklist)en tant qu'émetteur de SPAM et leurs envois étaient refusés par leurs interlocuteurs!

Il serait souhaitable que des centres de recherche se préoccupent d'analyser cette "industrie" car pour lutter efficacement contre ce fléau il est important d'en connaître les ressorts économiques et les points faibles. De premières informations provenant de Michel Ktitareff indiquent que différentes études menées aux USA indiqueraient qu'un taux de retour de 1 pour 100.000 suffit à rentabiliser l'opération (Les Echos 30 juin 2003) et que bêtise et curiosité, plus répendues que l'on ne pense, forment un riche terreau sur lequel prospèrent ces parasites

***le spam, ça pollue, mais ça marche**, selon l'étude de **Pew Internet & American Life Project** si 25 % des internautes se détournent de l'email et 70 % se plaignent...mais **un tiers** des sondés ont déjà cliqué sur un lien contenu dans un spam pour avoir plus d'infos, et **7 % d'entre eux ont commandé un produit par ce biais** Pew rappelle enfin que, l'année dernière, le spam représentait2 à 3 % du trafic global des emails. Cette année, le pourcentage monte à 55 % !* www.pewinternet.org/reports/pdfs/PIP_Spam_Report.pdf

*le magazine **Wired** www.wired.com/news/business/0,1367,59907,00.html rapporte que le site d'un spammeur **"Amazing Internet Products' websites"** présentait un défaut élémentaire de sécurité (cf affaires révélées par Kitetoa comme Tati) qui permettait de se faire une idée sur son "business model" (il suffisait de couper la fin de l'adresse pour accéder aux informations non protégées depuis la racine du site ce que l'on fait toujours si l'on est curieux et que l'on ne souhaite pas que le "clic" envoie au serveur les informations qui permettent de vous identifier :)*

*Ce site proposait des "**penis-enlargement pills" à 50$ la bouteille** et la "faille" permettait à tout internaute de voir que 6000 commandes en l'espace d'un mois avaient été reçues ... et fournissait **la liste complète des clients avec nom adresse, numéro de téléphone, n° de carte de crédit***

***Parmis ceux-ci** : le gestionnaire d'un fonds de pension (6 Milliards de $ de capitalisation, 2 bouteilles), le Pdg d'une entreprise aéronautique californienne membre actif du Rotary Club (6 bouteilles payées avec sa carte American express), le directeur d'une école de Pennsylvanie (4 bouteilles), le patron d'une institution financière, un chiropractor, un vétérinaire (pour ses clients?), un restaurateur célèbre, un paysagiste, plusieurs hauts gradés ... et de nombreuses femmes.*

***Les clients, contrairement à ce que l'on pourrait penser ne se recrutent pas seulement parmis les faibles d'esprit...** et pourtant pour commander il fallait fournir toutes ses données personnelles transmises en clair. A l'inverse, aucune adresse ni n° de teléphone ni même un e-mail n'était accessible au client*

*Seul élément de "crédibilité" de l'annonce "**vu à la télé**" (ce qui était de surcroit faux... mais l'enquête a montré que celà avait joué!)*

Bilan économique** : prix d'achat des bouteilles 5$, rémunération des "affiliés" qui expédient les Spam (et qui sont les seuls dans l'illégalité) 10$ par bouteilles vendues grâce à eux ... **résultat : un demi million de $ en un mois

*évidemment **le propriétaire officiel était une boite aux lettre** à Manchester (New Hampshire) avec un faux n° de tel et un faux e-mail. Les SPAMs étaient envoyées soit avec de fausses adresses de retour soit en usurpant l'adresse d'un internaute réel.*

***L'enquête** de Wired les a néanmoins conduit au propriétaire du site, champion d'échec de 19 ans vice-président de la New Hampshire Chess Association. Cette enquête a également montré que son "mentor" **Davis Wolfgang Hawke**, lui aussi champion d'échec et ex-néo Nazi était aussi depuis 1999 un "Maitre" reconnu dans le domaine du spam*

*Une question est-ce que au moins le produit est efficace? **Joe Miksch**, éditorialiste du Fairfield County Weekly dit avoir essayé. "premier jour pas de changement, deuxième jour pas de changement, troisième jour pas de*

changement, pour les jours suivants voir plus haut"... mais ***l'administration américaine*** *interrogée fait savoir qu'elle n'a pas pour autant les outils juridiques pour agir!*

3 Que faire contre le SPAM: les méthodes de première génération, parfois un remède pire que le mal

Progressivement, à défaut d'attaquer le mal à la source, faute de vaccins, se sont développés les techniques de protection: les filtres antispam, comme en son temps les filtres antivirus

Dans un premier temps il s'agissait d'une simple recherche de mots clé dans l'objet : viagra, porno, ... l'élargissement progressif du vocabulaire : girl, loan, Sildenafil Citrate, ... a commencé à se traduire par moult faux positifs (un échange récent au sein de plusieurs grands groupes m'a permis d'entre apercevoir l'ampleur des dégâts...) alors que dans le même temps les spammeurs se sont adaptés : V.I.A.G.R.A, V1AGRA, P0rno, "you forgot to reply", Help!, Your credit card has been charged for $234.65,... pour passer à travers les mailles du filet

Ce paragraphe transmis par messagerie par exemple a été considéré comme un spam par les systèmes primitifs mentionnés plus haut et qui continuent à être utilisés par de nombreuses entreprises: devant l'explosion du flux des spam qui passaient néanmoins à travers les mailles du filet les gestionnaires de ces outils ont simplement durci les critères (richesse du HTML utilisé, vocabulaire,..) sans réaliser que c'est la structure même de leur bouclier qui était devenue totalement inappropriée

Dans ce stade primitif ont été dressées des listes de spammeurs (**blacklist**) dont les mails ont été renvoyés à l'expéditeur, '**bouncés**' pour saturer leurs boites aux lettres: là encore la parade a été vite trouvée par les spammeurs avec des adresses de retour invalides et surtout des changements d'émetteur à chaque envoi.

Bien pire, comme nous le verrons plus loin, les spammeurs ont même, en excellents judokas**, retourné cette arme contre ceux qui l'utilisent** encore

4 Depuis l'été 2003, nouvelles technologies des spammeurs

Donc au début de l'été 2003, beaucoup poussaient un soupir de soulagement car ils avaient le sentiment que le problème était à peu près sous contrôle...

Mais catastrophe... en même temps que la canicule s'est progressivement développée une nouvelle stratégie des spammeurs (comme toujours les truands ont un coup d'avance sur la police!)

Nous voici confronté au gigantesque problème de la conjugaison entre les robots qui récoltent les adresses sur les sites, les virus qui vont les chercher dans vos carnets d'adresse et qui créent sur votre ordinateur, à votre insu des proxy server afin de les transmettre à l'extérieur,

Il s'agit notamment des virus de la famille ***Sobig*** *qui en était à sa version "F" en août 2003 et qui a réussi à contaminer au plus fort de son activité un message sur 17*

Des experts en sécurité redoutent que l'auteur des différentes moutures du ver frappe à nouveau, motivé par l'argent. Selon eux, il semble monnayer la liste des ordinateurs infectés auprès de spammeurs

«Tout a été très bien planifié, conçu et exécuté», a indiqué ***Mikko Hypponen****, directeur de la société* ***F-Secure****. Selon lui, il est probable que l'auteur du virus a monnayé la liste des ordinateurs infectés à des spammeurs. «Cette fois, nous sommes face à un virus créé pour une très bonne raison: l'argent»*

http://www.zdnet.fr/actualites/technologie/0,39020809,39116064,00.htm

Alan Ralski*, surnommé le* ***roi du Spam****, a déclaré avoir demandé à des développeurs roumains un nouveau vecteur de Spam permettant de contourner les firewall (p 260 du livre "les nouveaux habits du Spam" de Fréderic Aoun et Bruno Rasle* www.halte-au-spam.com

Non contents de vous spammer "au premier degré" (ce qui n'est plus bien grave car avec des filtres on arrive à peu près à les éliminer), les spammeurs usurpent maintenant souvent votre adresse pour

* **envoyer des spams** : outre quelques injures de personnes qui s'étonnent que des individus normalement fréquentables leur adresse de telles propositions, vous êtes submergés des "bounces" des vieux systèmes antispam et surtout des retours en erreur d'adresses périmées

* **envoyer des virus** : comme la plupart des destinataires bénéficient de filtres antivirus vous recevez un monceau de messages d'alerte des filtres de "vos" innombrables "correspondants" que le virus a, en votre nom, tenté de contaminer

d'après un article de www.lurhq.com/migmaf.html ***un spammeur aurait réussi à infecter des milliers d'ordinateurs grâce à un virus de type "cheval de Troie"*** *("wingate.exe" ou Migmaf) qui les dote d'un* ***proxy serveur web*** *et en "****déménageant" ainsi de proxy toutes les 10 minutes*** *: les pages appelées sont transférées à l'ordinateur piraté et de là appelées par le navigateur rendant impossible la localisation du "serveur maître". Pour appeler le serveur maître et afin de brouiller encore plus les pistes il génère un nombre considérable d'adresses dont une seule est la bonne, mais comment savoir laquelle (le serveur maître déménageant lui aussi régulièrement)*

Ce virus lui permet également d'envoyer son spam *depuis la machine piratée, se mettant ainsi à l'abri d'éventuelles mesures de rétorsion qui s'abattent sur sa victime*

Et là, votre **filtre anti Spam est totalement sans effet** sur ces messages d'erreur...: imaginons un envoi de 10 millions de spam sous votre identité dont 1% des adresses sont périmées et qui vous reviennent en erreur... (...or il ne vous en coûtera qu'une centaine de $ pour vous procurer une centaine de … millions d'adresses)

Le Washington post du 9 juin relate qu'un message intitulé "funny sexy screensaver" s'est retrouvé dans les boites aux lettre du gratin de la politique et de l'administration américaine avec comme adresse d'émission celle d'un ancien directeur de la CIA (cité par Mille Milliards d'e-mail, coédition Irepp Acsel sept 2002)

Beaucoup d'entreprises n'ont pas encore pris conscience de cette évolution nous et se spamment mutuellement à cause du détournement des armes mises en place lors de la guerre précédente et qui se retournent désormais contre elles: les spammeurs les prennent à leurs propres pièges en faisant **d'une pierre trois coups**

? La poursuite de cette stratégie vous prive de vrais messages (faux positifs) à cause du durcissement inapproprié de filtres structurellent inadaptés qui classe un message normal parmi les spam

? Elle vous vous conduit à être spammé par les victimes des vrais spammeurs : en faisant croire au système de défense de ces derniers que le message vient de vous, elle vous désigne comme cible pour leurs "bounce" contre lesquels vos protections sont sans effet (ce sont en effet des messages d'alerte "delivery error" de même type que ceux que vous recevez si vous faites une erreur sur le nom de votre destinataire ou si votre message était contaminé par un virus) : c'est ce que nous appellerons le "**rétroSpam**" qui représente un pourcentage de plus en plus grand des spams reçus et l'essentiel des nuisances aujourd'hui

? Elle risque de vous faire à tord **blacklister** car c'est vous qui êtes considéré comme à l'origine du Spam!!!

Tous ces SPAM **remplissent votre boite aux lettre** et bien vite celle-ci est pleine : vous perdez vos messages et votre correspondant reçoit un message d'erreur qui contribue à encombrer le réseau!

5 Un nouveau facteur de risque les logiciels "sociaux" de type Plaxo

S'y ajoute les logiciels "sociaux" de type Plaxo qui fonctionnent sur le mode du **virus belge**: rappelons que le virus belge vous explique comment détruire votre ordinateur en supprimant un fichier système (en vous le faisant prendre pour un dangereux virus) et en vous demandant de transmettre l'alerte à tout votre carnet d'adresse

De même **Plaxo vous demande de lui confier vous-même tout votre carnet d'adresse** (avec mail, téléphone, adresse physique,...) en vous offrant le service de le mettre à jour (ce qu'il fait, faut-il le dire, remarquablement bien), et, comme le virus belge, il vous utilise pour "spammer" vos correspondants en usurpant (avec votre accord) votre adresse pour leur proposer ses services.

Plaxo se constitue ainsi gratuitement un gigantesque fichier, avec la capacité de reconstituer les réseaux avec leurs centres d'intérêt.

La start-up a réussi à lever 2M$ en 2002 et encore 8,5M$ en août 2003, bien après la "bulle", or ses services sont gratuits, cela ne peut que rendre interrogatif sur son "business model".

"***there is no free lunch***" comme le rappellent **Fréderic Aoun** et **Bruno Rasle** *www.halte-au-spam.com* et ils soulignent l'extrême danger pour une entreprise de laisser ses cadres utiliser ce service car c'est en fait ainsi tout le carnet de clients et de prospects qui file dans un pays, certes ami, mais concurrent aussi

*" **Il y a plus inquiétant. Nous pouvons imaginer le scénario suivant** : Nous sommes en 2004, et la base de Plaxo compte **150 millions de contacts**…Un spammeur se procure un fichier d'un million d'adresses e-mail, non qualifiées et sans aucune autre information. Il s'abonne à Plaxo sous plusieurs comptes, et confie au système la mise à jour de ce fichier, présenté sous l'aspect d'inoffensifs carnets d'adresses Outlook. Très rapidement, notre spammeur se retrouve en possession d'un fichier enrichi des données personnelles relatives à chaque adresse : nom, téléphone, adresse physique…et ceci sans que les intéressés en aient été avertis ! Cette démarche est d'ores et déjà possible, le système étant autorisé par défaut à répondre automatiquement à une demande de mise à jour si la fiche est déjà gérée par Plaxo"*

*Outre le risque de piratage de la base ou de sa revente en cas de changement de contrôle de la société, Ils signalent que les transferts d'information de mise à jour adressés aux correspondants ne sont pas protégés et donc **aisément interceptables***

*le "**Phishing**", usurpant l'apparence d'un vrai questionnaire Plaxo peut en outre permettre des arnaques au second degré **Fréderic Aoun** et **Bruno Rasle***

De plus ce système nous paraît poser de sérieux problèmes juridiques: a-t-on le droit de transmettre un fichier nominatif avec des informations parfois très détaillées à un tiers (qui plus est dans un pays ou les règles de la privacy sont fort différentes des nôtres à l'insu du plein gré des personnes concernées?) Ceci parait contraire à l'article 14 de la directive européenne de 1995 et j'ai personnellement constaté que malgré une demande de retrait je continue à recevoir des demandes de mise à jour!.

La Belgique a interdit en mars 2003 toute collecte par parrainage

Notons (*www.pcmag.com/article2/0,4149,905467,00.asp*) que Plaxo a été développé par **Sean Parker**, un des fondateurs de **napster**

D'autres entreprises fleurissent sur ce modèle : **Spoke, AccuCard Service**, **GoodContacts**, **AdressSender, Friendster,…**

*Lancé en mars 2003, **Friendster** reprend une architecture peer to peer pour établir un contact avec «les amis de ses amis»: l'internaute crée son profil sur le site et doit ensuite rechercher une connaissance utilisateur du service. Une fois connectés, les deux internautes pourront accéder aux profils de leurs amis respectifs.*

Nous avons testé ce service: L'association directe (ou de premier degré) à deux amis proches nous ont permis d'accéder à un réseau de plus de 2.900 «amis» potentiels (allant jusqu'au quatrième degré) !

L'utilisateur peut effectuer des recherches en fonction de différents critères (affinités, sexe, age, etc.) ou simplement naviguer à travers les différents amis qui lui sont associés.

*Le service compte déjà **plus d'un million d'américains** avec 500 000 inscrits rien que pour le mois de juin 2003 et la croissance annoncée est de 20% par semaine .*

Malgré ses garde fous la base Friendster représente indéniablement une cible d'intérêt pour les spammeurs. Elle recèle non seulement des millions d'adresses e-mail mais également des informations de profiling très prisées des spammeurs sophistiqués.

Comme dans le cas des autres utilisant le parrainage, on peut se demander que deviennent les adresses e-mail de tous les filleuls (y compris ceux qui ne donnent pas suite à l'invitation) ? ***Frédéric AOUN et Bruno RASLE*** www.halte-au-spam.com

6 La nécessité d'employer des moyens beaucoup plus sophistiqués pour se protéger

Il a donc fallu passer à des systèmes beaucoup plus sophistiqués faisant appel à l'intelligence artificielle qui procèdent à une analyse structurelle fine et en tirent une "signature numérique" permettant de reconnaître un spam même s'il a subi des modifications.

Ce sont des systèmes qui fonctionnent par **auto apprentissage** : il faut leur donner chaque jour à analyser les spam qu'ils ont laissé passer ainsi que les faux positifs pour qu'ils apprennent à les reconnaître. Il faut donc une communauté nombreuse et disciplinée pour que ce système fonctionne efficacement

Bien entendu ces filtres ont un comportement "normand" : il est rare qu'ils répondent oui ou non : c'est toujours "peut être que oui, peut être bien que non" à 99%, 95%, 50%,...1%. C'est donc à vous de choisir l'équilibre entre les risques de faux positifs et de faux négatif, avec la possibilité d'une classe intermédiaire de "suspects" qui devra être triée à la main ...

Le réseau des anciens de l'Ecole Polytechnique durant l'été a éliminé 84% des spam sur 100.000 mails traités grâce au logiciel ***bogofilter*** *(avec un réglage excluant quasiment tous les faux positifs)*

L'Inria *annonce des scores supérieurs à 90% avec* ***SpamOracle****, spamassassin revendique des scores voisins...*

Ces scores se dégradent cependant parfois très vite avec l'évolution des techniques de spam et ils omettent souvent de compter les bounces de retrospam qu'ils reçoivent dans le décompte!

Il convient déjà de protéger les sites des **robots récolteurs d'adresse (harvesters),** d'autant plus que les gestionnaires des sites sont responsables juridiquement. La méthode à ce jour le plus efficace est de crypter ces adresses: elles restent visibles par un navigateur mais ne le sont pas par la génération actuelle des robots "harvesters" *voir un exemple d'utilisation de l'outil de cryptage mis à disposition par la CNIL http://www.yolin.net/test_cryptage_adresse.html*

Par ailleurs la nouvelle génération de virus conduit à recommander que **tout ordinateur connecté à Internet soit doté,** outre d'un antivirus mis à jour en permanence (un virus es surtout dangereux pendant les 3 premiers jours de son existence), d'un **firewall** afin d'éviter qu'un virus autorise un pirate à prendre le contrôle de la machine et s'en serve comme d'un émetteur de SPAM

7 Se défendre mais aussi attaquer le mal à la source…

Mais à l'évidence lutter contre ce fléau nécessitera, en dehors des mesures de protection (individuelles ou collectives), d'attaquer le mal à sa source de pénaliser économiquement les spammeurs ou de les faire condamner à des peines dissuasives

Il faudra pour cela coupler une **approche technique et une approche juridique** car une des difficultés principales est l'identification des spammeurs (les "fantassins", mais aussi les véritables responsables, ceux qui les manipulent et bénéficient de leurs services)

Certains proposent de faire payer l'envoi d'e-mail sous forme d'un **timbre électronique** payant pour dissuader les spammeurs en détruisant la rentabilité de leur modèle, avec en outre l'objectif de financer ainsi le développement de l'Internet en Afrique (avec une philosophie voisine de la "taxe Tobin"): l'idée est généreuse mais nous paraît totalement **irréaliste** (de plus elle ferait disparaître un des avantages majeurs du mail : sa simplicité. Malheureusement elle mobilise nombre de brillantes intelligences au détriment de propositions plus opérationnelles car, comme le rappelle Alexis de Tocqueville *"**une idée fausse mais claire a toujours plus de poids qu'une idée juste mais complexe**"*

Une proposition dérivée consiste à faire payer une **taxe en terme de temps de transmission** : en faisant résoudre un petit problème mathématique à la machine qui envoie le message, qui n'affecterait pas ceux qui envoient une quantité raisonnable d'e-mails, mais surchargerait le processeur d'un spammer (pour autant qu'il n'envoie pas ses spam à travers des milliers d'ordinateurs piratés…: La faisabilité paraît peu assurée)

Pour des mesures véritablement efficaces il nous semble qu'il faudra sans aucun doute envisager la création de nouvelles infractions et de certaines obligations pour les intermédiaires (on peut penser qu'il faudra s'inspirer des méthodes de lutte contre le proxénétisme, comme les lois réprimant le "proxénétisme hôtelier"),

Il faudra aussi vraisemblablement quelques amodiations des règles régissant le secret de la correspondance, ce qui est un sujet juridiquement particulièrement délicat (d'autant plus que cette lutte n'a de sens qu'au niveau international) mais il faut pour cela une étude technique pour déterminer le point faible à attaquer avec comme toujours un savant équilibre à préserver entre "privacy" et la sécurité (jusqu'ou accepter l'anonymat?)

La loi actuelle permet déjà de sévire quand les auteurs sont identifiés (car ils causent un préjudice en faisant supporter par d'autres des charges indues) : en 2002 un spammeur était condamné à verser **25M$** à son fournisseur d'accès (EarthLink) pour avoir expédié **plus d'un milliard de mails**. En 2003 ce même hébergeur obtenait d'Howard Carmack surnommé "Buffalo Spammer" une condamnation à lui verser **16M$** de dommages et intérêts pour avoir envoyé **825 millions de SPAM….** Mais cela n'a guère d'impact sur des spammeurs qui arrivent à cacher leur identité et l'analyse ci dessus montre que cela devient le cas général

Le Netizen Protection Act proposé par C Smith à la chambre des représentants n'est toujours pas voté (voir le site d'Eric Labbé spécialiste de la réglementation du spamming à l'université de Montréal *www.droit.umontreal.ca/~labee*, *www.digiplace.com/e-law*, *www.biozone.ml.org/juriscom* et *www.cauce.org*

*L'**Etat de Californie** l'a interdit, mais quelle portée pratique?, l'Etat de Washington a adopté une loi très sévère permettant de condamner l'expéditeur qui cache son nom ou le motif explicite de son envoi … mais encore faut-il*

mettre la main sur l'expéditeur réel…: la encore c'est essentiellement les PME débutantes qui risquent de se faire incriminer

Fin 2003 était en débat au Congrès US le Criminal Spam Act prévoyant des peines pouvant aller jusqu'à 5 ans de prison

L'Europe devrait en faire de même avec la directive du 12 juillet 2002 progressivement transcrite dans les droits nationaux (en France la loi déposée en juillet 2003 précise en son article 12 *: "Est interdite toute prospection directe, au moyen d'automates d'appel, télécopieurs ou courriers électroniques, de toute personne physique ou morale qui n'a pas exprimé son consentement préalable de recevoir de tels courriers"* *www.01net.com/rdn?oid=145481*. Mais là encore cet outil juridique suffira-t-il à arrêter les messages provenant des pays extérieurs à l'Europe?

la **directive européenne sur la e-vie privée du 31/10/2003** tranche pour "**l'optin**" (accord préalable) et interdit de camoufler l'identité de l'émetteur ou d'indiquer une adresse d'expédition non valable *http://europa.eu.int/information_society/topics/ecomm/highlights/current_spotlights/spam/index_en.htm*

La tentation est grande de prendre des réglementations extrêmement sévères pour satisfaire une opinion exaspérée par ces débordements mais qui serait dans la pratique totalement inapplicable. Une des premières difficultés sera de donner une définition juridique dépourvue d'ambiguïté au SPAM

Voir le dossier consacré à ce sujet lors du 3ème comité interministériel pour la Société de l'information, du jeudi 10 juillet 2003 : *www.ddm.gouv.fr/dossiers_thematiques/documents/cisi2003g6.html* , ainsi que *www.figer.com/publications/spam.htm* et *www.halte-au-spam.com*