

Spam – Le livre blanc

Etat de l'art

Table des matières

1. Origine du terme « spam »	4
2. A quoi sert le spam ?	4
2.1. Communication commerciale crapuleuse	4
2.2. Communication idéologique	4
2.3. Attaques par parasites, usurpation, ingénierie sociale...	5
2.3.1. Parasites viraux déployés par spam – le spam viral	5
2.3.2. Parasites viraux déployés pour zombifier vos PC	5
2.3.3. Parasites non viraux déployés par spam et machines zombies	5
2.3.4. Spam d'attaque	5
3. D'où viennent les spams ?	6
4. Que coûte le spam ?	6
5. Venir à bout du spam par la loi ?	7
6. Anti-spam idéal ?	7
7. Les causes de l'échec des solutions ordinaires	8
7.1. Echecs dus aux faux négatifs et aux faux positifs	8
7.1.1. Faux négatifs	8
7.1.2. Faux positifs	8
7.1.3. Conclusions	8
7.2. Echecs dus à l'élévation de la délation au rang de technique anti-spam	8
7.2.1. Délation	8
7.2.2. Conclusions	9
7.3. Echecs dus à l'élévation de la censure au rang de technique anti-spam	9
7.3.1. Censure commerciale	9
7.3.2. Censure politique ou idéologique	9
7.3.3. Conclusions	9
7.4. Echecs dus à l'usage de techniques de blocage faillibles	9
7.4.1. Échec des filtres sur les mots	9
7.4.2. Échec des filtres à règles d'évaluation (scoring ou « Intelligence Artificielle »)	9
7.4.3. Échec des filtres bayésiens ou filtres lexicaux	9
7.4.4. Échec des listes noires d'adresses e-mail des spammeurs	10
7.4.5. Échec des HoneyPots à calcul d'empreintes ou hashcode	10
7.4.6. Échec des listes noires d'adresses IPs	10
7.4.7. Échec des RBLs (Realtime Blackhole Lists) ou DNSRBLs	10
7.4.8. Échec des DNS MX Record Lookup	10
7.4.9. Échec des Reverse DNS Lookups	10
7.4.10. Échec des systèmes de destruction automatiques	11
7.5. Echecs dus à l'empilement des techniques	11
8. De l'échec comme argument publicitaire	11
8.1. Les solutions serveurs annoncent leurs échecs	12
8.1.1. Barracuda	12
8.1.2. CipherTrust – IronMail	12
8.1.3. Cloudmark – SpamNet	12
8.1.4. ICS Premium Anti-Spam	12
8.1.5. GFI MailEssentials 11	12
8.1.6. Symantec Mail Security 8200	12
8.1.7. MailControl Spam de BlackSpider	12

8.1.8.	Mail-Filters	12
8.1.9.	DMP – Dynamic Mail Processor de Dolphian	12
8.1.10.	Test du filtre antispam de Gmail (le WebMail de Google)	12
8.1.11.	Utilisateur de Hotmail ou MSN et Sender ID de Microsoft	12
8.2.	Les solutions client annoncent leurs échecs	13
8.2.1.	Spam-aware	13
8.2.2.	Vade-Retro (GOTO Software)	13
8.2.3.	G-Lock SpamCombat pour Windows 95/98/ME/NT/2000/XP	13
8.2.4.	SpamPal	13
9.	Quelle technologie anti-spam est fiable à 100% ?	13
10.	La technologie des « Test de Turing »	13
10.1.	Qui est Alan Turing ?	13
10.2.	Que sont les tests de Turing ?	13
10.3.	Que sont les tests de Turing appliqués à l’anti-spam ?	13
10.4.	Conditions économiques inacceptables pour les spammeurs	14
10.5.	Exemples de tests de Turing	14
10.5.1.	Challenges classiques	14
10.5.2.	Challenges cognitifs	14
10.5.3.	Challenges pour communautés à handicap disposant de matériel adapté	14
10.6.	Qu’est-ce qui accrédite la validité des tests de Turing ?	14
10.7.	Pourquoi les anti-spam à tests de Turing sont peu nombreux ?	14
10.8.	Quelles sont les solutions à base de tests de Turing ?	15
10.9.	La solution MailInBlack	15
10.10.	Le principe général de MailInBlack	16
10.10.1.	Première étape	16
10.10.2.	Seconde étape	16
10.10.3.	Troisième étape	16
10.10.4.	Quatrième étape	16
10.10.5.	Fin	16
11.	Ressources	17

Une étude publiée par Pew Internet le 10.04.05¹ confirme, une fois de plus, l'augmentation continue du spam malgré et contre les législations promulguées et les outils mis en place. On y décèle également une résignation certaine des internautes : aucune solution anti-spam ne semble satisfaisante.

Certains, encore plus alarmistes, comme le professeur Hannu H Kari, de l'Université de Technologies d'Helsinki, prédisent l'effondrement de l'Internet en 2006², entre autres à cause du spam.

Le problème est tel que les quelques dérisoires coups³ portés à un ou deux spammeurs⁴ et ⁵ sont montés en véritables spectacles par des éditeurs d'anti-spam plus soucieux de leur publicité et de la manne apportée par le spam que de tordre le coup une fois pour toutes à cette poule aux oeufs d'or.

1. Origine du terme « spam »

Spam - Épisode 1⁶ - jambon épicé en boîte « **S**piced **P**orc and **M**eat » depuis 1937 (existe toujours)

Spam - Épisode 2⁶ - 1970, une scène dans la première série du Monty Python's Flying Circus

Spam - Épisode 3⁶ - 5 mars 1994, Canter & Siegel inonde les groupes Usenet d'une publicité

Spam - Épisode 4⁶ - 12 avril 1994, un utilisateur de Usenet, excédé, lance :

«*Send coconuts and cans of **Spam** to Canter & Co. Be sure to drop the can of **Spam** on its seam first*».

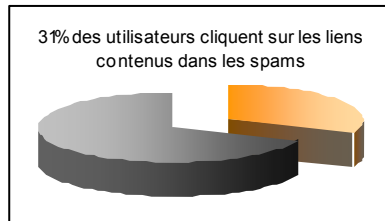
Le mot Spam qui désignait déjà le mauvais goût et les répétitions harassantes désigne désormais les correspondances non sollicitées.

2. A quoi sert le spam ?

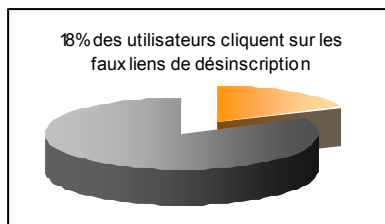
A vendre ! A vendre un produit ou un service ou à diffuser une idéologie...

Le spam arrive sur tous les ordinateurs, qu'ils aient une utilisation professionnelle ou familiale.

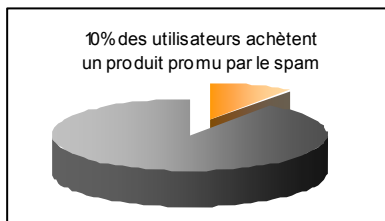
Il y a des spammeurs dont le but est simplement l'amusement : ils jouent à envoyer des courriers – n'importe quoi à n'importe qui – ce ne sont ni les plus nombreux ni les plus dangereux. Par contre, une analyse de la redoutable FTC⁷, aux États Unis, déclare que 96% des spams sont des offres, commerciales ou d'investissement, mensongères⁸. Pourtant, d'après une étude de Mirapoint-Radicati Group du 31 mars 2005⁹ (*chiffres significatifs bien que probablement « gonflés » par cet éditeur de solution anti-spam*) :



- » 31 % des spammés cliquent tout de même sur un des liens (*autre que le lien de désabonnement*) que contiennent ces spam. Pire : 10 % finissent par acheter le produit ou service vanté !



- » 18% des spammés sont trompés par les faux liens de désinscription, validant ainsi leurs adresses e-mail, accusant réception, par la même occasion, du spam ce qui permettra au spammeur de prouver son efficacité auprès de son commanditaire et, par la même occasion, de se faire payer son action de spam par l'annonceur publicitaire.



- » Plus de 10% de ceux qui ont suivi un lien contenu dans un spam poursuivent jusqu'à l'acte d'achat soit un taux de réussite de 3,1%. C'est un taux énorme en matière de publicité et incite des acteurs du e-commerce et leurs courroies de transmission, les spammeurs, à nous inonder de plus en plus!

Plus grave, la méthode de diffusion « classique » des spam¹⁰ est abandonnée au profit de méthodes fulgurantes avec la complicité, malgré eux, des internautes¹¹. Une convergence crapuleuse (*inaugurée par le virus¹² Mydoom le 26 janvier 2004¹³*) est confirmée entre les criminels auteurs de virus¹² et les spammeurs. Les techniques de spamming et les techniques de propagation des virus sont utilisées pour déployer, à l'échelle mondiale, des virus¹² invisibles qui transforment les ordinateurs de monsieur tout le monde en

relais à spam, confortant l'expansion continue des réseaux d'ordinateurs « zombifiés »^{14 15 et 16}.

2.1. Communication commerciale crapuleuse

Le fond de commerce du spam est la promotion commerciale mais aucune entreprise d'importance, ayant pignon sur rue, ne se lance dans cette activité. Les autres ne le font pas sur leur propre pays, la législation locale leur ferait prendre un trop haut risque. Le spam est donc essentiellement un outil commercial d'entreprises interlopes qui, depuis l'étranger, tentent le naïf et l'inexpérimenté avec des produits ou services miracles, fantaisistes, dangereux, interdits ou à contenus particuliers (élargisseurs de pénis, érections de 3 jours, travail au noir à domicile, chaînes d'argent, molécules pharmaceutiques, contenus pour adultes, sites pornographiques...). Tous ces acteurs appartiennent aux milieux des escrocs, du banditisme, de la crapulerie et des gangs maffieux. Le spam massif pro sites pour adultes est une plaie dans l'entreprise comme en contrôle parental. Certains gangs contrôlent plus de 40.000 sites pornographiques chacun dont ils font une promotion agressive par spam. A côté d'eux on trouve de très nombreux petits acteurs du spam, particulièrement ennuyeux car leurs « petites » action de spam pullules¹⁷.

2.2. Communication idéologique

- » Une association de parents d'élèves forte, en France, inonde ses adhérents de prises de positions politiques.
- » GovNet, aux États Unis, est une initiative de Washington d'intégrer les technologies d'information dans son arsenal militaire¹⁸, ce qui a donné, par exemple, une campagne de spams envoyés par l'armée américaine aux responsables civils et militaires irakiens, pour qu'ils cessent de soutenir le régime présidentiel de Saddam Hussein.
- » Peu avant la conférence internationale de l'OSCE (Organisation pour la Sécurité et la Coopération en Europe) consacrée à la relation entre la propagande raciste, xénophobe et antisémite sur Internet et les crimes inspirés par la haine, début juin 2004, une incroyable campagne de spams racistes¹⁹ rédigés en allemand et propagés grâce au virus¹² Sober²⁰, squattant les PC mal protégés des particuliers pour les transformer en serveurs de messagerie, à

inondé les boîtes e-mail transfrontières : les Français en recevaient jusqu'à 400 par jour sur chacune de leur boîte e-mail !

- » Attention : le communisme est de retour !²¹.
- » Le 18 mai 2005 le virus¹² Sober (variante Sober.Q), déjà cité, recommence avec des spams politiques rédigés en allemand à la gloire de l'extrême droite : « *Tu seras réduit en esclavage !* », « *Multiculturel = multiracial* », « *La Turquie dans l'Europe* », ...

2.3. Attaques par parasites, usurpation, ingénierie sociale...

2.3.1. Parasites viraux déployés par spam – le spam viral

Il y a les milliers de virus¹², anciens et nouveaux, totalement destructeurs, attachés en pièces jointes aux e-mail et que les débutants ouvrent en toute confiance. Ils ne le font qu'une fois et la leçon est vite apprise. Ces attaques brutales sont le fruit de jeunes apprentis sorciers, les « script kiddies », qui envoient des spams viraux tous azimuts et sans discernement.

Il y a les virus¹² qui ont besoin de votre machine et ne détruisent absolument rien. Le virus¹² Bagle²², par exemple, est déployé par spam. Le virus¹² Sober (variante Sober.N²³) déployé par spam, s'attaque, dans cet esprit, aux antivirus qu'il désactive.

Lorsque l'adresse de l'expéditeur semble être celle d'une connaissance (ami, collègue) grâce à une technique d'usurpation, ce serait 85% des internautes qui ouvrent la pièce jointe selon le site Tickbox.net²⁴ ! Nous sommes en présence du virus PEBCAK²⁵. La pièce jointe, oh combien utile à la correspondance électronique, est malheureusement devenue le sujet de toutes les angoisses dès qu'il s'agit de l'ouvrir.

2.3.2. Parasites viraux déployés pour zombifier vos PC

« Votre PC m'intéresse ! Je veux en prendre le contrôle et en faire l'un de mes zombies¹⁴ et ¹⁵ pour qu'il envoie mes spams sans que je me fasse repérer ! »

C'est ainsi que les mafias crapuleuses, dont les intérêts convergent avec ceux des mafias commerciales, détiendraient le contrôle de 30% des ordinateurs des particuliers dans le monde. Les

statistiques de Sophos publiées en mai 2005²⁶ observent : « Apparu à la mi-avril, Mytob-Z²⁷ est un programme particulièrement dangereux : non seulement il se diffuse largement, mais il installe également un cheval de Troie²⁸ qui ouvre une porte dérobée²⁹ permettant à des pirates de contrôler à distance l'ordinateur infecté. Ce dernier peut alors être espionné ou utilisé pour envoyer du spam ou des attaques par déni de service. »

2.3.3. Parasites non viraux déployés par spam et machines zombies

Le véritable problème des attaques de PC dans le monde n'est pas celui des virus¹² : les parasites utilisés sont beaucoup plus subtils et s'exécutent sans brutaliser les PC. Leur propagation est préférentiellement le mode « pièce jointe d'un spam » et ils servent à détourner l'usage des PC, à l'insu de leurs propriétaires, pour les transformer en zombies¹⁴ et ¹⁵ lanceurs de spam. Le spam pour mieux spammer ! Souvent classés, à tort³⁰, sous le vocable de virus¹², ce sont des chevaux de Troie³¹ dont la « charge active ou payload³² » est un serveur de messagerie (un serveur SMTP³³). Les gangsters du Net ont besoin de nos machines en bon état de fonctionnement. Ils pénètrent donc nos systèmes pour en prendre silencieusement le contrôle, sans se faire remarquer, sans rien détruire au passage. La prise de contrôle à distance d'un PC est connue de longue date et est pratiquée légitimement par bien des acteurs avec de nombreux outils commerciaux comme LapLink ou pcAnywhere³⁴. Pour les acteurs du côté obscur du Net, il n'en va pas de même :

- » Le spam pour mieux spammer. Les spammeurs ont besoin de PC pour envoyer leurs spams et transforment nos machines en zombies¹⁴ et ¹⁵ qu'ils équipent de serveurs de messagerie (serveurs SMTP). Plusieurs millions d'ordinateurs sont ainsi actuellement contrôlés par quelques spammeurs dans le monde et l'émetteur du spam devient intraçable. Le parasite utilisé est, lui-même, déployé par spams piégés. Selon l'éditeur d'antivirus Symantec³⁵, 30.000 nouveaux PC tomberaient ainsi, chaque jour, sous le contrôle de malfrats du Net. Selon l'éditeur d'antivirus Sophos³⁶, en février 2005, 30% du spam mondial est émis depuis des PC de particuliers contrôlés, à l'insu de leurs propriétaires, par les spammeurs.

« Les pirates semblent pénétrer des ordinateurs dans d'autres pays et utiliser ces PC "infectés" pour transmettre leurs messages ». « Certains chevaux de Troie et vers permettent en effet aux spammeurs de prendre le contrôle d'ordinateurs appartenant à des tiers innocents et de leur faire envoyer du spam. Plus de 30 % du spam émis dans le monde provient de ces PC, ce qui souligne la nécessité d'une approche coordonnée de la lutte anti-spam et antivirale. »

Le même Sophos poussait ce taux de 30% à 50% deux mois plus tard, en avril 2005³⁷.

« Sophos estime en effet que le mois dernier plus de 50% du spam émis dans le monde provenait d'ordinateurs "zombies"¹⁴ et ¹⁵, c'est-à-dire infectés à l'insu de leurs propriétaires par des pirates ou des auteurs de virus. »

- » Le spam pour piéger les données bancaires et financières. Les gangsters du Net ont besoin de vos données financières (comptes, codes, etc. ...) et implantent des keyloggers³⁸ ou des backdoors²⁹ grâce à des campagnes de spams piégés.
- » Le « London Action Plan » ou « Spam Enforcement Collaboration »³⁹ Les machines piégées, transformées en zombies¹⁴ et ¹⁵, sont devenues tellement nombreuses que le problème est désormais considéré par 30 agences gouvernementales et 17 groupes du secteur privé dans un cadre commun sous le vocable de « London Action Plan ». La redoutable FTC - Federal Trade Commission en fait partie ainsi que la Chine.

2.3.4. Spam d'attaque

- » Les délinquants en col blanc vont vous convaincre de leur donner vos références bancaires, codes, comptes, cartes, mots de passe, etc. ... avec des attaques par spam utilisant des techniques d'ingénierie sociale appelées Phishing⁴⁰.

- » Les médisants vont lancer, par spam, des rumeurs visant à attaquer untel ou untel. Ce peut être de la calomnie (voir Hoax⁴¹) mais ce peut être, également, une attaque appelée « Joe Job »⁴² contre un site Internet ou une personne.
- » Des escrocs spécialisés en blanchiment d'argent sale ou détournement de fonds publics vont tenter de vous appâter en vous faisant miroiter des gains fabuleux, en millions de dollars. Ces attaques par spam sont regroupées sous le vocable de Spam Nigériens⁴³.

3. D'où viennent les spams ?

1	Etats-Unis	35.70%
2	Corée du Sud	24.98%
3	Chine (& Hong Kong)	3.71%
4	France	3.19%
5	Espagne	2.74%
6	Canada	2.68%
7	Japon	2.10%
8	Brésil	1.95%
9	Royaume Uni	1.57%
10	Allemagne	1.23%
11	Australie	1.22%
12	Pologne	1.20%
13	Autres pays	11.73%

Figure 1- Classement Sophos du 12.05.05³⁷

Outre l'utilisation (à l'insu de leurs propriétaires) des ordinateurs des particuliers et des serveurs de messageries mal protégés des entreprises, certains spammeurs, pour envoyer leurs spams, disposent de leurs propres parcs de serveurs de messageries. Certains ont une puissance de feu supérieure à un milliard de spams par jour ! Le Spammeur Alan Ralsky⁴⁴, par exemple, dispose d'une puissance de feu de près de 3 milliards de spam par jour (190 serveurs à 650.000 spam à l'heure chacun !). Cette activité rémunératrice (il ne vend rien, il ne fait qu'envoyer des spam pour le compte de ses clients) lui permet de s'offrir une villa à 740.000 US\$⁴⁵ sur notre dos !

4. Que coûte le spam ?

« Envoyer 500 millions de spams coûte le prix d'un café »

Il est un autre problème que le risque de compromission de nos machines ou de notre vie privée par des parasites,

conduits ou non par le spam : c'est celui du coût du spam. Le spam coûte extrêmement chers. Contrairement au courrier traditionnel dans lequel l'émetteur paye un imprimeur, du papier, une enveloppe, la mise sous enveloppe, le paiement du service de distribution (affranchissement à la Poste...), le spam ne coûte strictement rien à l'émetteur : envoyer un spam à quelques millions d'exemplaires ne coûte rien, moins d'un euro, et encore... mais aurait rapporté 130 millions de dollars (en 2002 - chiffre probablement très sous-évalué lorsque l'on voit Intermix, auteur-éditeur d'un « adware », transiger à 7,5 millions de dollars pour éviter une condamnation à 2 milliards de dollars⁴⁶) aux spammeurs (le spammeur est la personne qui se charge, matériellement, de l'envoi du spam - à ne pas confondre avec le bénéficiaire du

peuvent rien à cause de la sacro-sainte inviolabilité de la correspondance privée. En France, Free, puis 9-Télécom (mars 2005), ont intégré des solutions anti-spam à « profil bas » configurables uniquement par le FAI (nous verrons d'ailleurs plus loin que les solutions anti-spam ordinaires mises en place côté serveurs sont des catastrophes à interdire).

- » Tous les utilisateurs finaux perdent un temps précieux, lors de la réception de leur courrier, à trier le bon grain de l'ivraie et ce temps représente de l'argent, surtout en entreprise.

En 2003 le coût du spam est estimé à 20 milliards de dollars dans le monde selon les études, séparées mais convergentes, de l'Union Européenne et de Ferris Research, à San Francisco⁴⁷ et double chaque année⁴⁸.

Le spam coûterait aux employeurs près de 2.000 dollars par an et par salarié ! Selon un rapport de Nucleus Research, il a coûté 1.934 dollars par an et par salarié en 2004 contre 874 dollars en 2003⁴⁹. La perte de productivité annuelle du salarié est de -3,1% en 2004 (contre -1,4% en 2003), Le spam fait perdre, en moyenne, à chaque employé, 14,5 minutes par jour en 2004 (contre 6,5 minutes en 2003) sur son temps de travail. D'autres études parlent de 10 à 20 minutes par jour et par employé connecté. Aucune solution anti-spam ordinaires n'étant fiable à 100%, ces coûts, risques et temps perdus perdurent même après investissements dans des anti-spam et du personnel (informatique ou non).

Début mai 2005, l'institut Radicati Group estime que les spams représenteront, d'ici 2008, 71% des menaces (spam, virus¹², chevaux de Troie,...) et qu'ils coûteront aux seules entreprises européennes quelque 85 milliards d'euros au cours de ces quatre prochaines années. Cette étude est confortée par une nouvelle publication du même groupe⁵⁰, le 30 juin 2005 : le spam en Europe va croître de 54% par an durant les 4 prochaines années et constituera 71% de tous les messages reçus en Europe.

Déjà en 2003 un article de synthèse du New York Times⁵¹ était alarmant et concluait sur une perte de 3 milliards de dollars uniquement à cause des faux positifs (les spam non détectés par les outils ordinaires anti-spam) en sus des 650 millions de dollars investis en outils anti-spam ordinaires achetés par les entreprises et des 85 milliards de dollars perdus en « temps perdu » !

- » Tous les intermédiaires (serveurs de messageries acheminant le message de l'émetteur vers le destinataire) supportent des coûts : de stockage et de charge processeur conduisant à l'implantation de nouveaux équipements, de facturation de leur surconsommation de bande passante, d'embauche de personnels informaticiens supplémentaires... Les chiffres font état de 50% du trafic mondial sur l'Internet occupé par le transit de spam. Postini, éditeur de solution anti-spam, estime que la part des spams dans la circulation de messages sur le Net atteint 87% ! IDC estime le nombre de spams, par jour, à 12 milliards ! Les FAI (Fournisseurs d'Accès Internet) sont excédés mais ne

5. Venir à bout du spam par la loi ?

- » C'est une gageure. La législation la plus dure et la plus récente, aux États-Unis, s'appelle « Can-Spam Act⁵² », c'est-à-dire : « Pouvoir spammer » !
- » Le président de la FTC⁵³ (équivalent de la DGCCRF française⁵⁴) a déclaré : « ...même si je suis d'un naturel optimiste, je ne peux dire que je pense que nous viendrons à bout de ce problème juste par l'application de la loi... ».
- » Shimon Gruper, directeur des technologies Internet d'Aladdin Knowledge Systems, interrogé sur TF1 le 31 octobre 2004 disait, à propos des effets attendus de l'entrée en vigueur de la directive européenne interdisant le spam : « Bien peu d'effets, malheureusement. Pas un texte de loi ne pourra faire quelque chose pour arrêter les spams. Un courriel indésirable a souvent été envoyé depuis l'étranger, et même s'il est envoyé depuis la France, il a très bien pu transiter par un serveur situé dans un autre pays. Je pense que la seule motivation de tels textes de lois est de pouvoir dire "on a fait quelque chose contre cette nuisance" ».
- » En France, la prise de position de la CNIL (Commission Nationale de l'Informatique et des Libertés), le 17 février 2005, en faveur du spam des salariés⁵⁵ a provoqué des remous dans le Landernau de la sécurité et de la lutte anti-spam. Cette prise de position concerne l'interprétation de la Loi pour la Confiance dans l'Economie Numérique (LCEN) et libère de manière importante la prospection B to B (Business to Business). Elle suppose, en sus du spam, la constitution de fichiers d'adresses e-mail et l'utilisation de tracking et profiling⁵⁶ préalable à l'aide de techniques de type spywares⁵⁷.
- » Les dispositions françaises de la LCEN (Loi sur la Confiance dans l'Economie Numérique) sont totalement inefficaces et inapplicables⁵⁸, la quasi-totalité du spam venant de l'étranger et se moquant de notre législation. Simultanément, certains craignent que cette même législation bloque la communication et donc le développement des entreprises françaises.
- » Les industriels constatent l'incapacité des préoccupations légales et s'unissent pour tenter de définir un standard qui n'arrive

pas à émerger : ce projet, sous le nom de JEAG pour Japan E-mail Anti-abuse Group, regroupe, notamment, NEC, IBM Japan, Yahoo Japan, Nifty, Softbank...

- » Totalement ubuesque : un internaute victime de spam et qui le refusait se voit demander 3,8 millions de dollars de dommages et intérêts par un spammeur !⁵⁹.

6. Anti-spam idéal ?

L'anti-spam idéal est l'outil qui rejette 100% des courriers non sollicités (et des pièces jointes contenant des virus¹² et autres parasites) et accepte 100% des correspondances légitimes. Ce n'est que doté d'un tel anti-spam idéal qu'un utilisateur peut se permettre :

1. d'ouvrir sans crainte tous ses courriers légitimes entrant
2. de demander sans crainte la destruction automatique de tous les autres courriers

Dans la pratique, aucune des solutions anti-spam habituelles n'approche, même de très loin, cet idéal. Toutes ces solutions génèrent des faux positifs (courriers jetés alors qu'ils sont légitimes) et des faux négatifs (courriers légitimes jetés).

Toutes les solutions anti-spam ordinaires réduisent donc à néant les espérances de :

1. disparition du risque de compromission
2. économie de temps
3. économie d'argent
4. retrouver une productivité normale

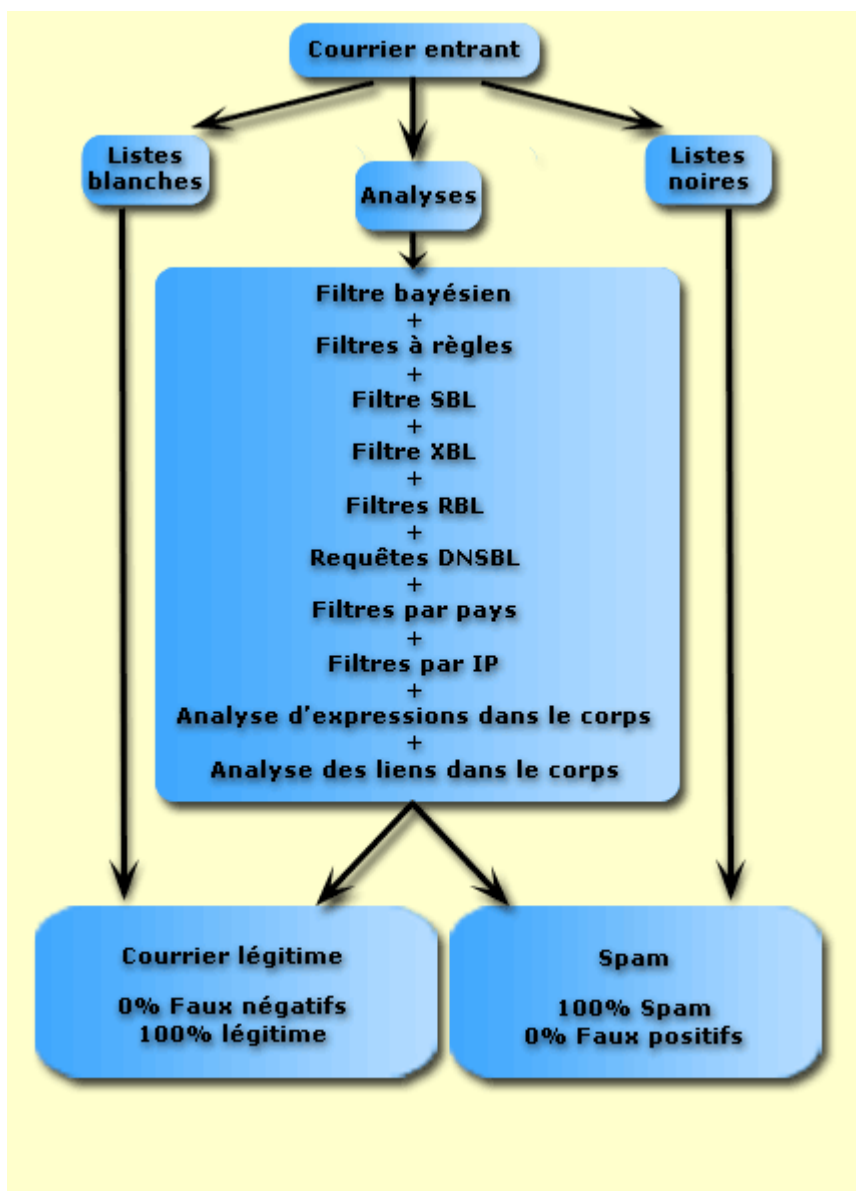


Figure 2- Anti-spam ordinaire idéalisé

Une seule approche de l'anti-spam donne satisfaction et peut être qualifiée d'anti-spam idéal : l'usage des tests de Turing.

Il saute aux yeux que ces solutions « ordinaires » idéalisées sont constituées d'un incroyable empilement de filtres (et encore n'avons nous pas représenté les filtres antivirus) qui sont, chacun, un programme, parfois d'une inextricable complexité. Certains éditeurs de solutions anti-spam ordinaires font de cet empilement, qui accouche de solutions à la taille monstrueuse⁶⁰, un argument publicitaire alors que les faiblesses des uns et des autres ne s'annulent pas mais, au contraire, s'amplifient !

Les énormes taux de faux positifs et de faux négatifs de ces usines à gaz (et quand bien même ces taux seraient infimes) rendent les solutions anti-spam « ordinaires » complètement inexploitable **en confiance**, donc sans intérêt.

7. Les causes de l'échec des solutions ordinaires

7.1. Echecs dus aux faux négatifs et aux faux positifs

L'une des raisons majeures de l'échec des solutions anti-spam ordinaires réside tout simplement dans leur taux d'erreur, admis mais inadmissible. Il suffit d'une seule erreur, même à l'état potentiel, pour que l'on ne puisse pas faire confiance au produit et qu'il faille continuer à vérifier de visu toutes les réceptions. Or, la très sérieuse revue PC Expert, en son numéro de mai 2005, page 123, déclare : « pas de parade totalement efficace » « mais habilement combinées, elles peuvent permettre de bloquer 90% des spams ». Remarquons que cet article n'aborde pas la technique anti-spam des Tests de Turing.

7.1.1. Faux négatifs

Un seul spam passant au travers de la solution anti-spam peut compromettre toute la confidentialité ou la sécurité d'un système et oblige l'utilisateur à ne jamais se reposer sur sa solution anti-spam. Il peut s'agir de tracking et profiling commercial, de phishing, de virus¹², de l'implantation d'un backdoor²⁹, de l'implantation d'un serveur SMTP mettant l'ordinateur au service d'un spammeur, de l'implantation d'un client de calcul distribué mettant les ressources de la machine au service de réseaux crapuleux...

Le Journal du Net, le 24 avril 2005⁶¹, publie une étude américaine sur les filtres anti-spam : 10 à 20% de dommages collatéraux ! « *Revers de la médaille des filtres anti-spam, une partie des e-mails sollicités n'atteignent jamais leur destinataire. Une proportion moyenne*

évaluée à 22 % par Return Path. ». Presque le quart des messages commerciaux légitimes (opt-in) seraient donc totalement perdus, essentiellement à cause des filtres anti-spams côté serveurs de messagerie. Le traitement anti-spam doit se faire côté client !

7.1.2. Faux positifs

Un seul faux positif (courrier légitime classé par erreur en spam) oblige l'utilisateur à ne jamais se reposer sur son anti-spam, à ne jamais détruire automatiquement ce qui est classé en spam et à lire sa boîte à spam pour en extraire son courrier légitime jeté ! Un devis, une commande qui passe à la trappe et c'est une sérieuse mise à mal de la solution anti-spam et par là, de la confiance dans le service informatique de l'entreprise.

7.1.3. Conclusions

Si une technique génère un seul faux positif ou un seul faux négatif, l'utilisateur ne peut pas se reposer sur elle !

7.2. Echecs dus à l'élévation de la délation au rang de technique anti-spam

Une autre grande raison de l'échec des solutions anti-spam ordinaires vient de la participation, volontaire ou forcée, des internautes eux-mêmes, dans d'incroyables réseaux de dénonciations.

7.2.1. Délation

Une grande partie de la classification des correspondances en spam est obtenue par la mise en place de systèmes de délation dans lesquels il est fait appel aux internautes pour dénoncer les spams. Les éditeurs de solutions anti-spam ordinaires ont mis en place des pages permettant de

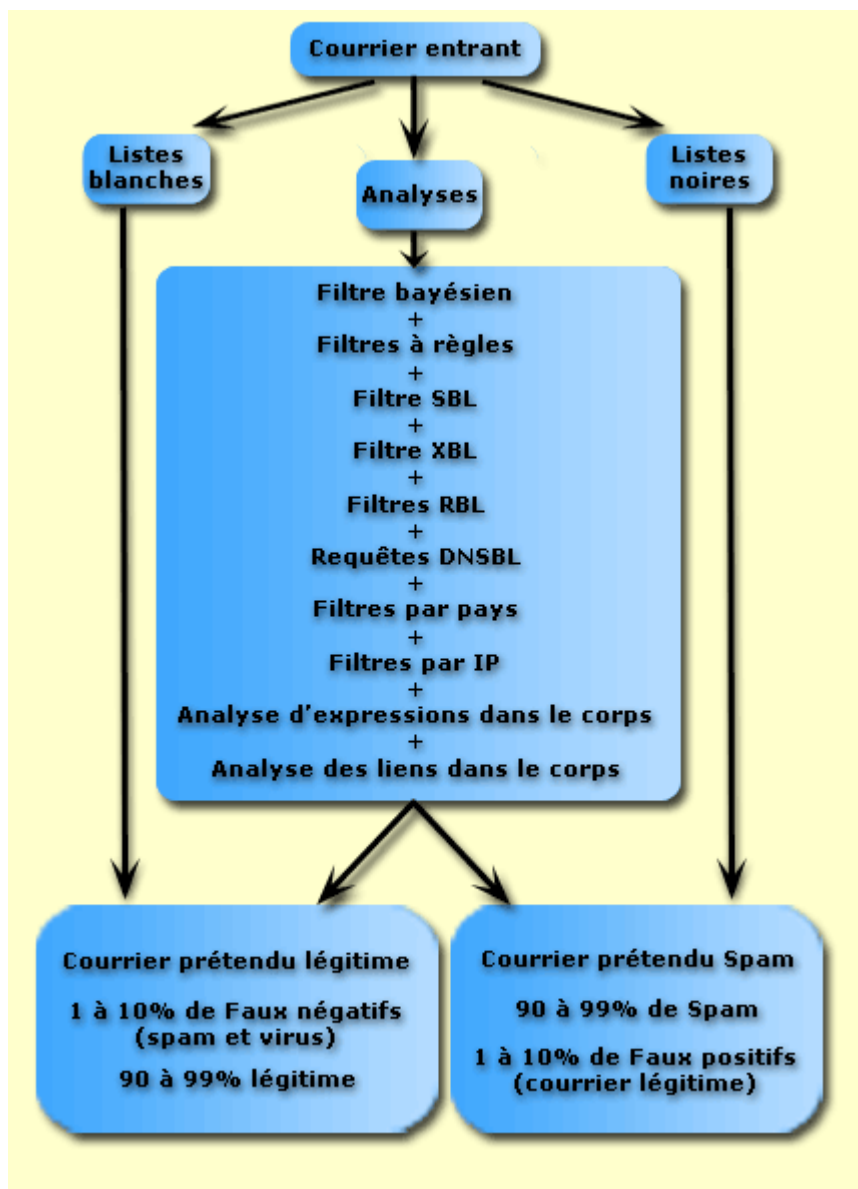


Figure 3- Anti-spam réel

dénoncer, souvent de manière anonyme, tel e-mail comme étant un spam, SpamCop⁶², par exemple.

A partir d'un seuil de dénonciation (par exemple une vingtaine de dénonciations), le texte (le corps) de l'e-mail est signé (calcul d'un chiffre clé, son hashcode, type MD5⁶³) et cette signature, telle la signature d'un virus¹² dans un antivirus, est insérée dans la base de connaissance de l'anti-spam.

Ceci à ouvert la porte aux fausses dénonciations (concurrences commerciales etc. ...).

7.2.2. Conclusions

Il n'est jamais bon de se reposer sur les autres pour porter un jugement sur sa propre correspondance or le Net permet à des nébuleuses anonymes, par ce biais de la délation, de biaiser les algorithmes des solutions anti-spam ordinaires.

7.3. Echecs dus à l'élévation de la censure au rang de technique anti-spam

Certains « organismes » anti-spam sont complètement inféodés à un gang de e-commerce ou à une idéologie et dévoient le système en s'érigeant en censeurs du Net. Les outils anti-spam, pour tenter d'être efficaces, se servent simultanément de plusieurs listes publiques de blocage. Plusieurs de ces listes ne sont pas honnêtes. Les internautes ne sont pas du tout avertis de ces déviations.

7.3.1. Censure commerciale

Le cas de la nébuleuse SpamCop/IronPort. SpamCop, un site de lutte contre le spam, est connu pour ses listes ouvertes de blocage de spammeurs (RBL – Real-time Black List). IronPort est connu pour ses machines réputées être les plus rapides à envoyer du courrier – elles sont appelées « canon à spam » car elles sont souvent acquises par des spammeurs. D'un autre côté, IronPort est un acteur de la lutte anti-spam ce qui lui a valu un article dans le New York Times du 25 novembre 2003, titré « Une société arme les 2 camps dans la guerre du spam ». Justement, ce 25 novembre 2003, IronPort achetait SpamCop et y injectait 1 million de US\$. Justement, les RBL de SpamCop contenaient le blocage de nombreux serveurs de clients de la société IronPort. Malheureusement SpamCop bloque régulièrement des concurrents d'IronPort en matière d'anti-spam... SpamCop illustre bien l'une des raisons de l'échec des solutions ordinaires : être juge et parti⁶⁴. (ps : le 15 juin 2005, Trend, éditeur d'antivirus qui se lance dans l'anti-spam, rachète la société Kelkea et ses RBL).

7.3.2. Censure politique ou idéologique

AOL manipule politiquement son anti-spam. Le célèbre prestataire donne dans la censure et bloque, par exemple, tous les e-mails contenant un lien vers le site contestataire bushin30seconds.org⁶⁵

7.3.3. Conclusions

Les solutions anti-spam ordinaires peuvent vous manipuler à votre insu.

7.4. Echecs dus à l'usage de techniques de blocage faillibles

Le simple fait d'être amené à utiliser plusieurs techniques pour tenter de bloquer les spam prouve que les techniques utilisées sont, chacune en ce qui la concerne, insuffisante et faillible.

7.4.1. Échec des filtres sur les mots

Le camouflage des mots qui pourraient faire réagir les filtres à mots est un sport joué avec maestria par les spammeurs. Vous pouvez toujours demander à classer en spam les e-mails contenant le mot

viagra

dans le sujet ou dans le corps mais, allez-vous créer des filtres pour toutes les formes d'écritures que les spammeurs peuvent donner à ce mot afin de circonvenir votre filtre ?

Viagra

(le v majuscule n'est pas un v majuscule mais un \ suivi d'un /),

vIgra

(ce n'est un « i » mais un « l »),

**vi@gra, v,i,a,g,r,a,
vi,a,gra,ViAGRA,...**

Il y a quelques milliers de déclinaisons, uniquement sur ce mot. Recommencez ensuite avec les centaines de mots normalement bloquant, à décliner en milliers de formes chacun. Voici les 25 premiers autres mots les plus utilisés par les spammeurs :

**cialis, orgams, viagra,
shipping,milf, valium,
pharmacy, xanax, increase,
vicodin, orgasm, online,
disclaimer, rolex, required,
remove, prescription,
hydrocodone, guaranteed,
cheap, adobe, ambient, free,
price, discount**

Quant-aux spam rédigés dans des alphabets non latin (chinois, japonais, cyrilliques, grecques, arabe etc. ...) aucune solution anti-spam n'est multilingue.

Les filtres à mots sont des échecs totaux. Pire, ce sont des filtres impossibles⁶⁶ ! Enfin, ils provoquent des faux positifs (un e-mail adressé à un médecin et parlant de ces produits n'a pas à être bloqué !).

7.4.2. Echec des filtres à règles d'évaluation (scoring ou « Intelligence Artificielle »)

Ces filtres sont plus élaborés que les filtres à mots bien qu'ils soient également basés sur la recherche d'occurrences de mots. Au lieu de bloquer purement et simplement une correspondance sous prétexte qu'un seul mot figurant dans une liste de blocage s'y trouve, ils attribuent un score, un nombre de points à chaque mot clé ainsi trouvé. Ils le font également pour le contenu de l'entête (la partie cachée d'un e-mail) et les points peuvent être positifs ou négatifs. Par exemple, un mot imprononçable dans aucune langue aura un score négatif très élevé, la présence d'une adresse de réponse identique à l'adresse d'envoi aura un score positif, la présence de mots comme « désinscrire » ou « désinscription » ou « désabonnement » aura un score négatif comme la présence des mots « cliquez ici » ou « achetez » ou « discount » (surtout si ces mots sont en capitales) etc... A la fin, plus le score est négatif, plus le courrier a des chances d'être un spam. SpamAssassin ou SpamPal sont des exemples de solutions anti-spam ordinaires utilisant massivement ce type de filtres à règles d'évaluation.

Les spammeurs sont actifs et ont très vite circonvenu ces filtres en masquant les mots-clé par diverses techniques (« Snowflaking » ; « Noise words » (bruit de fond) ; « HTML tricks » (balises malformées...) comme les déclinaisons dactylographiques ou l'encapsulation des mots « à risque » dans une image... Une nouvelle technique est apparue récemment : le spam en Ascii Art. C'est un document en texte pur (ce n'est pas une image). Il n'éveille pas l'attention des outils anti-spam car les lettres sont formées de la juxtaposition de signes « normaux » (un calligramme). Voir l'illustration⁶⁷.

7.4.3. Échec des filtres bayésiens ou filtres lexicaux

Les solutions bayésiennes sont personnalisées à chaque utilisateur. Ce sont typiquement des solutions adaptables à chaque personne physique et complètement inadaptées aux solutions anti-spam côté serveur. Il s'agit d'une magnifique construction intellectuelle, à phase d'apprentissage, basée sur des calculs de probabilités. Elle donne uniquement des résultats probables, sans

aucune certitude. Le taux de réussite est, en moyenne, de 90% à 95%. Ces solutions bayésiennes sont des échecs totaux⁶⁸ en usage personnel où ils ne peuvent échapper aux faux positifs et aux faux négatifs. Pire que tout, le battage médiatique autour de ces filtres auréolés de mathématisme et de scientisme les a fait adopter dans des solutions ordinaires côté serveur où il fait bon dire que l'on a un filtre bayésien alors que ce n'est pas du tout sa place !

7.4.4. Échec des listes noires d'adresses e-mail des spammeurs

Comment a-t-on pu concevoir un tel filtre ? Comment peut-on promouvoir une telle technique et crier haut et fort en disposer sans craindre le ridicule ? Il faut vraiment méconnaître le monde du spam. Les adresses des spammeurs, lorsqu'elles sont réelles, sont des adresses jetables. Elles sont sur des domaines « poubelles » comme HotMail. Elles n'ont de durée de vie que celle de chaque campagne de spam soit environ 1 semaine. Le prochain spam, en provenance du même spammeur, n'aura aucune adresse commune avec ses précédents spams. Mais, dans 99,9% des cas, l'adresse prétendue du spammeur est usurpée (et bien réelle) grâce aux centaines de milliers de zombies¹⁵. Ce sont donc des milliers d'adresses e-mail légitimes, dont parfois celles de votre cercle de connaissances, qui apparaissent dans ces spam. Le contenu de cette liste noire est donc imbécile. Sa taille devient vite immense. Le temps de balayage de cette liste à chaque courrier reçu est indigeste à nos ordinateurs et vis-à-vis des administrateurs informatiques.

Autre impossibilité de mettre en œuvre ces listes : beaucoup de listes de diffusion auxquelles nous sommes abonnés n'utilisent pas d'adresse e-mail d'émetteur (From :) pourtant ces correspondances sont légitimes. Mais alors, quid des spam dans lesquels les spammeurs ne mettent pas d'adresse From : ? Ils tombent dans la légitimité ou nos abonnements tombent dans la boîte à spam ?

7.4.5. Échec des HoneyPots à calcul d'empreintes ou hashcode

Les adresses e-mail « Pots de miel » (Honeypots) sont volontairement exposées pour capter un maximum de spam. Ces adresses ne peuvent recevoir que du spam et rien d'autre. Par exemple, une adresse réelle est cachée dans un site Web. Personne ne la connaît. Elle n'a jamais été utilisée ni publiée ou donnée à qui que se soit. Elle ne peut être utilisée que si un robot capteur d'adresses e-mail, envoyé par un spammeur, l'a trouvée. Le but est de calculer instantanément les

chiffres clé⁶³ (hashcode) ou les empreintes (signes caractéristiques) des corps de ces messages, obligatoirement non sollicités.

Les spammeurs ont immédiatement trouvé la parade : si vous regardez bien vos spam, il y a toujours, quelque part, une espèce de code aléatoire qui fait que jamais 2 spam identiques n'ont de signatures de type hashcode identiques (ou les corps du message est personnalisé au nom du destinataire...).

7.4.6. Échec des listes noires d'adresses IPs

Les blacklists sont une technique répandue de blocage des spam. Elles occupent assez peu de temps du processeur et sont aisées à implémenter. Elles nécessitent un important travail manuel de maintenance de ces listes contenant les adresses IP des serveurs des spammeurs connus. Les e-mails en provenance de ces serveurs sont bloqués.

Malheureusement, les spammeurs changent régulièrement de serveurs et donc leurs adresses IPs changent tout le temps. Ils sont parfois, pour les très gros gangs, leurs propres « registrar ». Ils disposent en propre de plusieurs vastes intervalles d'adresses IPs sur lesquelles ils font « tourner » des serveurs légitimes afin de « dé-blacklister » leurs adresses IPs.

Les Blacklists sont donc utiles pour tenter de bloquer, assez rapidement, un envoi massif qui se ferait depuis une seule adresse IP donnée. Elles ne peuvent s'inscrire dans une lutte anti-spam de fond, sur la durée (il faut les mettre à jour, manuellement, en permanence – faire entrer et sortir des adresses). Elles sont complètement impuissantes contre les spam fulgurants utilisant des centaines de milliers de zombies. Enfin elles sont entre les mains d'organisations, plus ou moins bénévoles, dont les buts sont parfois entachés de concurrence déloyale ou d'auto proclamation « censeurs du Net ». Leur temps de réaction, pour sortir une adresse introduite par erreur, est très long, augmentant le nombre de faux positifs.

7.4.7. Échec des RBLs (Realtime Blackhole Lists) ou DNSRBLs

Inventaires automatisés des listes noires d'adresses IPs et des noms de domaines des spammeurs connus ou présumés. Elles fonctionnent comme des DNS et, de ce fait, occupent assez peu de ressources processeur. Elles provoquent plutôt beaucoup de faux positifs compte tenu d'une certaine « agressivité ». Des domaines entiers sont blacklistés puis les émetteurs légitimes sont déblacklistés un par un, après analyse de leur plainte, jusqu'à trouver le coupable. Une mise à jour toutes les ½ heure est un minimum,

voire toutes les 10 minutes. Les RBLs publiques sont généralement soumises à un droit d'accès payant (abonnement) mais certains éditeurs (Brightmail, Trend, Aladdin, Clearswift...) s'appuient sur leurs propres RBLs. Les RBLs proposent également des listes de serveurs mal protégés pouvant être utilisés en relais par les spammeurs – des robots parcourent le Net et sondent les serveurs de messageries à la recherche de vulnérabilités les rendant disponibles aux usurpateurs (les spammeurs disposent des mêmes robots pour chercher des serveurs à pirater).

7.4.8. Échec des DNS MX Record Lookup

Cette technique, qui ralentit énormément la réception des correspondances et sature les réseaux consiste à regarder si l'adresse prétendue de l'émetteur (partie gauche d'une adresse e-mail) et l'adresse prétendue de réponse existent bien sur le domaine prétendu d'émission (partie droite d'une adresse e-mail). On pratique donc un DNS Lookup qui consiste à demander l'autorisation à un serveur de messagerie d'envoyer un message sur une adresse e-mail. Si celui-ci répond « Ok » c'est que l'adresse e-mail existe réellement. Il est bien entendu que le « spoofing » et les zombies rendent sans effet cette technique anti-spam.

7.4.9. Échec des Reverse DNS Lookups

Cette technique, qui ralentit énormément la réception des messages et sature les serveurs DNS, recherche un nom de domaine à partir de son adresse IP. Si le domaine trouvé correspond au domaine (partie droite) de l'adresse e-mail de l'émetteur prétendu, l'e-mail est acceptable pour cette règle.

Cette technique génère un taux de faux positifs considérable car les DNS ne fonctionnent pas tous en reverse DNS ou sont mal paramétrés ou sont volontairement silencieux. En sus, beaucoup de noms de domaines sont dit « de vanité » (noms commerciaux achetés, qui « sonnent » bien... C'est le cas de tous les e-mails émis par toutes les petites sociétés et les particuliers qui préfèrent acheter un nom de domaine plutôt que d'utiliser le nom de domaine de leur fournisseur d'accès Internet (FAI – ISP) ou de leur hébergeur) mais ne correspondent pas du tout au nom de domaine réel du serveur. Dans tous ces cas, les e-mails sont rejetés alors qu'ils peuvent être légitimes.

Notons que c'est dans la voie de l'amélioration de ces Reverse DNS Lookups que s'engouffrent toutes les grandes manœuvres actuelles de l'anti-spam ordinaire :

- » Reverse Mail Exchanger (RMX)⁶⁹
- » Sender Permitted From (SPF)⁷⁰
- » Designated Mailers Protocol (DMP)⁷¹
- » Yahoo! Domain Keys⁷²
- » Microsoft Caller ID for Email (maintenant "Sender ID")⁷³

7.4.10. Echec des systèmes de destruction automatiques

Pour faire une erreur de temps en temps, il faut un homme. Pour faire plusieurs millions d'erreurs à la seconde il faut un logiciel or il n'existe pas de logiciel 100% sans erreur. La solution pour serveurs de GFI, MailSecurity, a effacé tous les messages, y compris les correspondances légitimes, de tous ses clients, durant 24 heures⁷⁴ ! On ne peut - on ne doit jamais - demander à une solution anti-spam ordinaire de détruire automatiquement les courriers classés comme spam et on ne doit jamais autoriser les mises à jours automatiques de logiciels⁷⁵ ! A cause du risque d'erreur des solutions anti-spam ordinaires, l'utilisateur doit impérativement vérifier sa boîte à spams, a fortiori si la solution est une solution serveurs dans laquelle strictement aucun courrier ne doit être détruit !

7.5. Echecs dus à l'empilement des techniques

L'empilement des techniques dans le même anti-spam n'améliore pas forcément son taux d'échec, aussi faible soit-il, mais accouche de monstres consommant de trop importantes ressources machine. En sus, chaque technique emporte ses propres failles et croire que l'une pallie les faiblesses de l'autre relève de l'aveuglement ou de la méthode Coué.

On en arrive à un tel empilement de techniques en échec que des délires intellectuels invraisemblables sortent des chapeaux ! Des chercheurs de l'Université de Californie et de l'Université de Floride veulent rendre les logiciels anti-spam plus efficaces en leur permettant d'échanger des informations (toujours la course, perdue d'avance, derrière l'interdit). Lorsque les filtres « classiques » seront incapables de déterminer si un

email est un spam, ils enverront des requêtes auprès des logiciels anti-spam d'autres internautes connectés. Si, à leur tour, ils n'arrivent pas non plus à classer le message en spam ou légitime, ils enverront eux aussi des requêtes à d'autres internautes connectés, et ainsi de suite. Plus cette architecture comprendrait d'utilisateurs et plus le filtrage du spam serait efficace.

C'est complètement fou. Cela oscille entre la compromission du système par la délation (faux positifs intentionnels), la saturation des réseaux, le détournement du système par les spammeurs et la faille de sécurité que représente ce type de connexions. D'autres projets du même genre existent déjà dans CloudMark (une série de logiciels partagent les informations des usagers pour détecter le spam) ou le projet SpamWatch, qui, lui aussi, se basera sur un réseau p2p. On trouve également ce genre d'approche dans le service SpyNet de Microsoft Antispyware.

L'implantation de solutions anti-spam ordinaires, multicouches, ralenti de manière drastique la vitesse de délivrance des courriers et la capacité de production, des autres programmes installés sur les mêmes machines. Il s'agit donc d'un poste de coûts plutôt que d'économies. Simultanément, le taux d'erreur des solutions ordinaires ne permettant pas de se reposer dessus, aucun gain de temps n'est constaté et le coût de gestion du spam reste le même, voire augmente. On note, par contre, une augmentation du risque par le relâchement de la vigilance qu'entraîne la confiance accordée à tort à de tels outils.

- » Les anti-spam ordinaires entraînent une mobilisation gigantesque des ressources des machines à cause d'algorithmes de plus en plus complexes et de plus en plus nombreux empilés les

uns sur les autres. Les temps de réponse des ordinateurs s'allongent à chaque réception d'une correspondance. Un test a été conduit sur une machine puissante (processeur à 3Ghz et 1Go de ram). La relève des messages à lieu toutes les 5 minutes (4 à 8 messages chaque fois en moyenne). La machine est équipée d'un anti-spam ordinaire, SpamPal. Un écroulement complet des temps de réponse de l'ordinateur est constaté à chaque relève du courrier, avec ralentissement intolérable des autres applications qui sont quasiment suspendues. Ceci est dû au temps calcul nécessaire à tous ces filtres empilés.

En outre, le classement automatique en spam et la destruction automatique, par ces anti-spam ordinaires, peut être totalement contraire à des intérêts bien compris : de quel droit un outil bloquerait les spams des concurrents d'une société alors que le service marketing tient absolument, au contraire, à les recevoir et les analyser, tandis que le service du personnel ne le souhaite pas ? De quel droit un outil bloquerait la correspondance d'un médecin parce que le mot Viagra y figurerait ?

Enfin, jamais un filtre anti-spam ordinaire ne doit être installé côté serveur de messagerie mais uniquement côté poste client.

8. De l'échec comme argument publicitaire

Il est délicieux de lire les communiqués de presse des éditeurs de solutions anti-spam ordinaires : ils insistent tous sur le fait que leur solution laisse passer très peu de spam et génère très peu de faux positifs. Autrement dit, toutes ces solutions annoncent, à grand renfort de publicité,

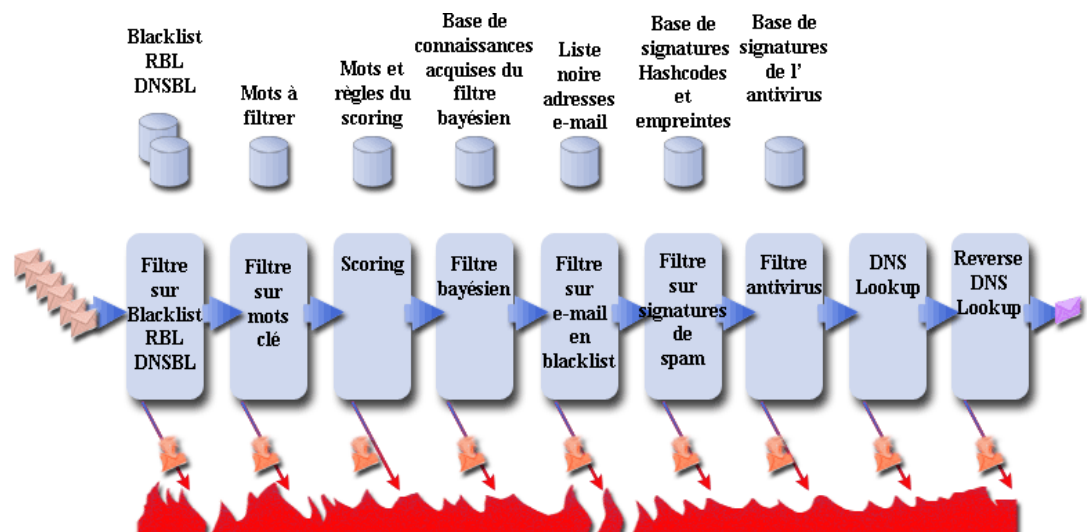


Figure 4- Anti-spam ordinaire

qu'elles ne fonctionnent pas ou qu'elles fonctionnent mal !

Mirapoint, fournisseur de solutions de sécurité et de serveurs de messagerie et InfoSecurity Europe ont publié, le 12 mai 2005, une enquête sur l'incidence du contrôle anti-spam sur la fiabilité de la messagerie⁷⁶. Quelque 60 % des personnes interrogées déclarent qu'un filtre anti-spam a bloqué certains messages légitimes qu'elles auraient dû recevoir ! 42 % reconnaissent avoir manqué une échéance à cause de ce problème ! C'est un véritable drame pour l'entreprise comme pour l'utilisateur.

8.1. Les solutions serveurs annoncent leurs échecs

Vu du côté de l'intéressé, l'internaute au bout de la chaîne, les solutions anti-spam sont nombreuses et, parfois, gratuites, mais il existe également toute une panoplie d'outils anti-spam pour les administrateurs de serveurs de messagerie.

Outre le fait que ces solutions ne soient pas fiables et que leurs éditeurs soient fiers de l'annoncer, de quel droit un serveur de messagerie interfère-t-il avec ma correspondance privée ? De quelle autorité et de quelle intelligence se croit-il doté pour s'ériger en censeur de ma correspondance ?

Les conséquences de tels actes peuvent être catastrophiques (commandes clients, devis... qui disparaissent sans aucune possibilité de récupération...).

Le 3 mai 2005 les abonnés d'AOL habitant la Floride ont vu les e-mails provenant du service d'alerte des ouragans de l'Etat de Floride être supprimés par le logiciel anti-spam installé par leur Fournisseur d'Accès Internet⁷⁷.

Les utilisateurs de Verizon, un des plus gros fournisseurs d'accès américain avec 3 millions d'abonnés ADSL, se plaignent du nombre élevé de messages qui ne leur parviennent jamais du fait des filtrages opérés par leur prestataire⁷⁸. La situation est d'autant plus gênante que l'expéditeur ne reçoit pas de message lui signalant que son message n'est pas arrivé à destination. Pire, Verizon a choisi de bloquer, purement et simplement, tous les e-mails en provenance de toute l'Europe, la Chine et la Nouvelle Zélande, y compris les comptes gouvernementaux ! En France, un facteur qui bloquerait une seule lettre serait jeté en prison ! Verizon est d'ailleurs poursuivi en justice par ses clients⁷⁹. Jamais une solution anti-spam ordinaire, ne gérant pas le filtrage des comptes individuellement et sous l'exclusif contrôle du propriétaire du compte, ne doit être installé côté serveur.

Quelques exemples d'annonces publicitaires d'échecs, côté serveurs !

8.1.1. Barracuda

« Notre taux de faux positifs est l'un des plus bas »⁸⁰. En sus, ils se fendent de cette incroyable publicité : « Pour chaque faux positif, l'émetteur reçoit un message en retour lui disant que son message n'est pas arrivé ». Donc, ils savent que c'est un faux positif et ils ne délivrent pas le message légitime ! Ils expliquent même cela dans un document⁸¹ où l'on peut penser que leurs messages envoyés aux expéditeurs constituent du spam et polluent le réseau Internet. Une étude⁸² montre que leur taux de faux positifs est de 0,3 pour 100 et le taux de faux négatifs de 6 pour 100 !

8.1.2. CipherTrust – IronMail

Un papier de CipherTrust, en mars 2005, déclare que le challenge⁸³ des éditeurs de solutions anti-spam est d'essayer de diminuer le taux de faux positifs ! Essayer seulement de diminuer le taux ! On ne parle pas du 100% sans erreur qui est définitivement inaccessible à toutes les solutions anti-spam ordinaires.

8.1.3. Cloudmark – SpamNet

Ce système est un mélange de solution client et de solution serveur. Il fait remonter l'intégralité des correspondances rejetées manuellement par ses utilisateurs vers leurs serveurs (*le dispositif incorporé dans Outlook et Outlook express peut être considéré comme une faille de sécurité*) et prétend ainsi avoir atteint le niveau zéro en faux positifs⁸⁴. En réalité ils sont en juin 2004 à 17 faux positifs sur 1032 soit 1.65% (une autre étude⁸⁵ de septembre 2003 les gratifie de 14,9% de faux négatifs) et 37 faux négatifs sur 2035 soit 1,81% !⁸⁶

8.1.4. ICS Premium Anti-Spam

14.04.05 : Ipswitch intègre la technologie anti-spam de Mail-Filters.com⁸⁷. Que lit-on sur le site de Mail-Filters.com⁸⁸ : « intercepte 95% du spam avec moins de 1 faux positif par million de messages »

8.1.5. GFI MailEssentials 11

06.04.05 : « GFI MailEssentials 11 a associé plusieurs technologies réagissant dans la minute dans sa lutte contre les spammeurs, afin d'arriver à avoir un taux de détection de plus de 98% ». Déclaration de David Vella, Directeur du Développement des produits à GFI Software⁸⁹.

8.1.6. Symantec Mail Security 8200

27.03.05 : « Cette offre permet ainsi de garantir le plus haut niveau de protection grâce à un filtrage optimal des e-mails en supprimant 95% des spams avec un taux de faux positifs le plus bas du marché

(99,9999%) (messages légitimes ayant été classés dans la catégorie spam). »⁹⁰.

8.1.7. MailControl Spam de BlackSpider

12.10.04 MailControl Spam stoppe les e-mails spam à plus de 98%⁹¹.

8.1.8. Mail-Filters

Il ne s'agit pas d'un produit en lui-même mais d'outils commercialisés auprès d'éditeurs d'anti-spam (appliance matériel ou solutions logicielles) qui les intègrent dans leurs solutions. On peut donc les retrouver dans plusieurs solutions. Ils annoncent fièrement un taux d'échec de 5% et un taux invérifié de faux positifs de 1 pour 1.000.000⁹².

8.1.9. DMP – Dynamic Mail Processor de Dolphian

« dmp est spécialement conçu pour minimiser le nombre de faux-positifs »⁹³... Cependant l'éditeur ne fourni aucun chiffre concernant ce taux de faux positif.

8.1.10. Test du filtre antispam de Gmail (le WebMail de Google)

Test du 07.02.05 au 07.03.05 par spamfo.co.uk. Sur 404 e-mails reçus, 15 faux négatifs et 11 faux positifs !⁹⁴

8.1.11. Utilisateur de Hotmail ou MSN et Sender ID de Microsoft

Dans les grandes manœuvres pour dominer le Monde, Microsoft tente d'imposer sa solution, « Sender ID »⁹⁵ (fusion des systèmes SPF¹⁰⁵ et ¹⁰⁶ de Meng Weng Wong et Caller ID for E-mail de Microsoft). Il déclare aux possesseurs de serveurs de messagerie : « A partir de novembre 2005, utilisez Sender ID⁹⁵ sinon vos courriers seront considérés comme du spam ! ». Les dommages collatéraux (messages légitimes jetés) vont être sans commune mesure avec les 10% d'erreur des solutions anti-spam ordinaires. Si Microsoft met sa solution, bancale, non reconnue⁹⁶ et contre laquelle⁹⁷ s'élèvent bien des avis, en œuvre, pour la faire admettre de force comme un standard « de fait », la perte de messages légitimes va être considérable et pourrait atteindre 90% à 100% de la correspondance – actuellement moins de 0,3% des plus grandes entreprises américaines a incorporé cette technologie (le Sender Policy Framework - SPF). En sus, cette technologie a connu une hémorragie de ses membres, l'année dernière, après le refus de Microsoft d'autoriser son utilisation dans les applications en open source. D'autre part, cette technologie bloque certaines fonctionnalités du Web comme les services de redirection ou du

type "Envoyer à un ami" proposés par de très nombreux sites. C'est le moment de rappeler qu'il n'est jamais recommandé d'utiliser une boîte aux lettres HotMail ou MSN – voilà une occasion d'en changer – d'autant que « Sender ID » est déjà contourné par les spammeurs qui légitiment leurs serveurs dans les bases « Sender ID » tout simplement en les y inscrivant. Etc...

8.2. Les solutions client annoncent leurs échecs

Quelques exemples :

8.2.1. Spam-aware

Un taux d'efficacité supérieur à 95% soit 5% de faux négatifs !⁹⁸.

8.2.2. Vade-Retro (GOTO Software)

95% de spam en moins soit 5% de faux négatifs !⁹⁹. Solution limitée à Outlook et Outlook Express. Solution également utilisée côté serveur (Free.fr par exemple avec son service minimaliste¹⁰⁰).

8.2.3. G-Lock SpamCombat pour Windows 95/98/ME/NT/2000/XP

Communiqué de presse du 03.03.05 : « Bien formé, G-Lock SpamCombat est capable d'arrêter 99,5% du spam »¹⁰¹.

8.2.4. SpamPal

Considéré comme la meilleure solution anti-spam gratuite, SpamPal a été testé ce printemps 2005 durant 2 mois sur l'une de nos machines. SpamPal jette tous les jours des courriers légitimes et attendus dans la boîte à spam et laisse passer des spams, malgré des réglages draconiens. L'assouplissement des réglages ne fait qu'aggraver le problème. Le taux de faux positifs est d'environ 10%, de faux négatifs d'environ 0,1%.

9. Quelle technologie anti-spam est fiable à 100% ?

A la lecture des pages précédentes prouvant les carences avérées des solutions anti-spam ordinaires, il apparaît que seule une solution s'appuyant sur un Test de Turing (Challenge Response) soit imparable.

Comme en beaucoup de domaines, il faut « réfléchir autrement ».

La totalité des solutions anti-spam ordinaires évoquées plus haut, qu'elles soient côté serveur ou côté client, passent leur temps à courir derrière l'interdit et, par conception et essence, ont donc toujours un temps de retard ou une technologie de retard sur les spammeurs.

La créativité des spammeurs est actuellement sans limite et oblige à

l'empilement des filtres, un par idée géniale des spammeurs pour contourner nos barrières ! Aujourd'hui, les solutions anti-spam nécessitent tellement de puissances de calcul qu'elles commencent à migrer du poste client vers le serveur ce qui est une pure aberration : l'anti-spam ordinaire, côté client, a au moins pour lui d'être paramétré en fonction du profil de son utilisateur et le filtre bayésien dont il est équipé fait son apprentissage en fonction de la spécificité de la correspondance de son utilisateur. Aucun anti-spam côté serveur ne peut être personnalisé pour autant de profils d'utilisation qu'il y a de comptes à protéger. Seuls des paramètres génériques ne satisfaisant personne peuvent être appliqués sur les solutions anti-spam côté serveurs.

Les éditeurs de solutions anti-spam ordinaires accouchent donc de véritables usines à gaz pour un piètre résultat : la simple probabilité, à 90%, que tout le courrier classé spam en soit réellement. Cette faible probabilité leur suffit pour décider de détruire définitivement et silencieusement ce « probable » spam, sans en avertir le destinataire ! Pourtant, ils n'ont aucune certitude sauf la certitude d'être, au moins à 10%, dans l'erreur !

De quel droit un bête logiciel décide à la place de l'internaute et jette, là bas, au loin, côté serveur, sans aucune possibilité de récupération, des correspondances, parce qu'elles ont simplement de fortes chances d'être du spam ? Autant jouer à la roulette russe !

Une longue réflexion sur le principe d'inversion de la charge a conduit aux anti-spam avancés, exploitant la technologie des « Tests de Turing » : l'esprit dans lequel ces anti-spam avancés sont est totalement opposé à l'esprit des anti-spam ordinaires :

« Au lieu de courir derrière ce qui est, peut-être et sans aucune certitude, du spam, intéressons-nous à ce qui est, avec certitude, légitime. »

10. La technologie des « Test de Turing »

10.1. Qui est Alan Turing ?

Turing Alan Mathison¹⁰² :

Mathématicien, logicien et informaticien britannique, il fut l'un des fondateurs de l'informatique moderne, avec Von Neumann John et Wiener Norbert. Il émet les concepts de La Machine de Turing, en 1936 : c'est la théorie de la calculabilité. Il s'agit de formaliser le principe d'algorithme, représenté par une succession d'instructions agissant en séquence sur des données d'entrée susceptible de fournir un résultat. Les

ordinateurs actuels, votre ordinateur, sont encore entièrement basés sur l'architecture des machines de Turing. Alan Turing contribue grandement à la victoire de la bataille de l'Atlantique en perçant, grâce à sa méthode, le secret d'Enigma, le système de chiffrement des Allemands durant la seconde guerre mondiale (39-45). C'est en 1950 qu'il énonce son célèbre Test de Turing.



Alan Turing

10.2. Que sont les tests de Turing ?

Historiquement, c'est un jeu basé sur des travaux antérieurs qui cherchaient à déterminer le sexe d'une personne rien qu'en discutant avec elle par écrit (sans la voir, sans l'entendre). Puis, ce test a été étendu à la détermination de l'"humanité" de l'interlocuteur. Celui-ci est-il un humain ou un robot parlant, comme Alice ? Est-ce que l'ordinateur pense ? On met un expérimentateur-testeur d'un côté, et on cache une machine ou un humain de l'autre. Si le testeur se fait avoir par une machine et ne sait pas faire la différence entre l'homme et la machine, alors la machine pense.

Ce test se résume à une expérience dans laquelle un observateur tient une conversation avec un tiers inconnu. Comment cet observateur, par l'unique analyse des messages échangés, pourra-t-il distinguer l'homme de la machine ?¹⁰³

10.3. Que sont les tests de Turing appliqués à l'anti-spam ?

Il s'agit de s'assurer de l'humanité d'un émetteur de courrier électronique : est-ce bien un humain ou est-ce un robot ? Pour ce faire on va demander à l'expéditeur du courrier (la seule première fois où il écrit à quelqu'un protégé par un test de Turing) de faire quelque chose qu'un robot ne sait pas faire (ou ne peut pas faire dans des conditions économiques acceptables pour l'émetteur).

On va lui demander de résoudre une énigme, simplissime pour l'humain, impossible pour la machine, raison pour laquelle certains tests de Turing s'appellent « Challenge Message » ou « Captcha » (Completely Automated Public Turing test to tell Computers and Humans Apart). S'il y a une réponse satisfaisante, on considère l'émetteur comme réellement humain. Son adresse e-mail est alors placée automatiquement en liste blanche et sa correspondance sortie automatiquement de la file d'attente (quarantaines). Il ne lui sera plus demandé de prouver son humanité.

Dans tous les autres cas (mauvaise réponse ou pas de réponse du tout), l'émetteur n'est probablement pas légitime, a moins qu'il soit en déplacement ou en vacances. Sa correspondance est stockée automatiquement en liste d'attente, appelée « quarantaine », pour une durée paramétrable (par exemple 40 jours soit un peu plus que l'absence normalement la plus longue de quelqu'un). Ce n'est qu'à l'issue de cette période que la quarantaine est automatiquement purgée des plus anciens courriers dont aucun humain n'a revendiqué l'envoi.

Bien entendu, l'utilisateur protégé par un test de Turing peut jeter un œil sur le contenu de sa file d'attente et en sortir une correspondance avant que l'expéditeur n'ait eu à résoudre l'énigme.

10.4. Conditions économiques inacceptables pour les spammeurs

Le test de Turing repose sur une énigme visuelle très simple à résoudre pour l'humain : découvrir un mot ou une suite de caractères, généralement distordus, disposés sur un fond perturbé. Le cerveau humain détecte ce qu'il faut révéler instantanément. Le spammeur, à qui serait renvoyés des milliers ou millions de tests de Turing, devrait développer un logiciel de reconnaissance de caractères d'une telle puissance que le coût en deviendrait inacceptable pour lui.

D'autres Tests de Turing peuvent être utilisés, visuels, cognitifs, auditifs, pour répondre à des besoins particuliers (malvoyants...) ou de goût.

- » Résoudre un puzzle
- » Identifier un objet ou un animal en photo
- » Choisir un intrus dans une liste de mots
- » Etc. ...

10.5. Exemples de tests de Turing

La plupart des tests de Turing reposent sur la demande de copie d'un code dont l'écriture est déformée et s'affiche sur un

fond irrégulier, de manière à empêcher l'utilisation de logiciels de reconnaissance de caractères. En voici 7 exemples, utilisés par AOL Instant Messenger, ICQ, Yahoo!, PayPal, Microsoft Passport etc. ... Il en existe même en braille pour protéger les ressources Internet destinées aux malvoyants.

10.5.1. Challenges classiques

La figure 5 ci-dessous illustre quelques exemples de challenges classiques.

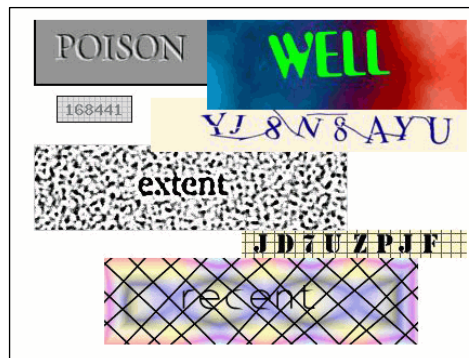


Figure 5 : Challenges classiques

10.5.2. Challenges cognitifs

Un test de Turing comme le suivant est dit « Cognitif ». La question est choisie au hasard ou est fabriquée à la volée, à partir d'une base de données de plusieurs milliers de questions ou d'informations ordonnées.

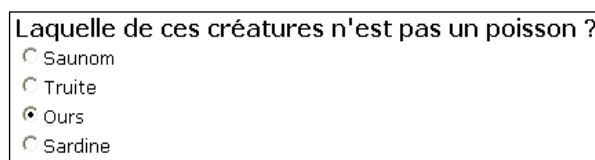


Figure 6 : Challenges cognitifs

10.5.3. Challenges pour handicapés à matériel adapté



Figure 7 : Challenges adaptés

10.6. Qu'est-ce qui accrédite la validité des tests de Turing ?

On rencontre la preuve de la validité de cette solution partout et tout le temps sur le Net. Toutes les activités Internet qui

risquent d'être attaquées par un robot se sont protégées avec ce système ultime et ont implémenté des tests de Turing. Vous les avez déjà rencontrés à plusieurs reprises. Ils vérifient votre « humanité ».

- » Lorsque vous vous inscrivez sur un site, celui-ci vous envoie un e-mail et vous demande d'y répondre pour valider votre inscription. C'est un test de Turing (simple).
- » Lorsque vous vous inscrivez sur un forum, l'administrateur envoie un e-mail de validation auquel vous devez répondre. C'est un test de Turing simple (servant simultanément à vérifier l'exactitude de votre adresse e-mail).
- » Depuis la vague d'attaques en cyber-squatting de 2003/2004 par des gangs de e-commerce maffieux de l'Est, la plupart des forums de discussion se protègent en vous demandant, à l'inscription, de recopier un code aléatoire apparaissant dans une image et en vous envoyant un e-mail auquel vous devez répondre. C'est un test de Turing.

» La solution anti-spam réseau FairUCE¹⁰⁴ d'IBM vérifie l'adéquation entre l'adresse IP d'expédition et le nom de domaine (et intégrera SPF¹⁰⁵ et ¹⁰⁶ si SPF arrive à être standardisé). IBM avoue que l'ultime solution est le Test de Turing qu'il incorpore dans FairUCE¹⁰⁴ en cas de doute.

10.7. Pourquoi les anti-spam à tests de Turing sont peu nombreux ?

Il y a plusieurs raisons à cela :

- » Si la technique est ancienne, elle n'est utilisée en ce domaine que depuis très peu de temps.
- » Les chercheurs en anti-spam ordinaires sont obnubilés, aveuglés par la chasse à l'interdit. Ils s'y sont engouffrés, emboîtant le pas aux méthodes antivirales¹⁰⁷ et anti-spywares¹⁰⁸ ordinaires à base de signatures. Les éditeurs de solutions anti-spam ordinaires sont d'ailleurs, souvent, des

- croissances des éditeurs d'antivirus et ils reproduisent, dans ces nouveaux outils, les méthodes qui sont les leurs depuis 20 ans : les bases de signatures et les blacklists... Rappelons que dans le monde des antivirus¹⁰⁷ et des anti-spywares¹⁰⁸ existe le même cas de figure avec les systèmes de contrôles d'intégrité¹⁰⁹, peu nombreux et hautement plus performants, partant de la même démarche : « au lieu de courir après les virus¹², trojans¹¹⁰, spywares¹¹¹ et autres parasites malsains pour tenter de les reconnaître (bases de signatures...), intéressons-nous à la préservation de ce qui est légitime et sain ».
- » Les investissements sont devenus tellement énormes qu'il n'est plus possible aux éditeurs de solutions anti-spam ordinaires de faire marche arrière et de changer radicalement de stratégie industrielle et commerciale. C'est comme si un éditeur d'antivirus¹⁰⁷ ou d'anti-trojans¹⁰⁸ à base de signatures et d'analyses heuristiques abandonnait tout pour passer à un système intellectuellement complètement inverse, bien que plus performant : « le contrôle d'intégrité¹⁰⁹ ».
 - » Les tests de Turing posent aux éditeurs d'anti-spam ordinaires plusieurs problèmes : ils sont simples, scandaleusement simples, outrageusement efficaces, et rendent la gestion de la correspondance à leurs propriétaires, les internautes. Ceci est impensable pour ces multinationales dont le métier est d'exister par de nouvelles technologies brevetées et secrètes, véritables trésors industriels et donc commerciaux. En outre ces sociétés se saborderaient complètement, d'un point de vue marketing, en avouant qu'elles se sont fourvoyées dans des technologies impasses.

10.8. Quelles sont les solutions à base de tests de Turing ?

Il en existe quelques-unes. La plupart sont américaines, non traduites, et souffrent de divers faiblesses :

- » Absence de traitement antivirus
- » Obligation d'utiliser un WebMail et d'abandonner son outil de messagerie favori
- » Changement de son adresse e-mail

- » Nécessité d'installer un logiciel côté client
- » Dépendance vis-à-vis d'un client de messagerie ou deux, sans portabilité possible
- » Dépendance vis-à-vis d'un système d'exploitation
- » Faiblesse du test de Turing utilisé qui pourrait être mis à mal par un logiciel d'OCR
- » Solutions criminelles proposées par certains pour se constituer des listes d'adresses e-mail validées et vendues à des spammeurs, voire solutions proposées par des spammeurs ! Voir Spam Arrest¹¹²
- » Non comptabilité avec un serveur de messagerie (type Exchange, Domino, etc. ...)
- » Système impersonnel et/ou abrupt

10.9. La solution MailInBlack

Une seule solution, particulièrement bien pensée, emporte tous les suffrages au niveau mondial et incorpore tous les points forts des Tests de Turing sans aucun des défauts d'implémentation rencontrés ailleurs. MailInBlack est la première solution qui garantit l'élimination de 100% des spams et des virus¹² connus transmis par e-mail, sans aucun risque de perte de messages légitimes et sans aucun travail d'administration !

- » Test de Turing dur
- » Compatibles avec 100% des clients de messagerie actuels et à venir (indépendance totale)
- » Compatible avec 100% des systèmes d'exploitation (indépendance totale)
- » Existence de solutions client – MailInBlack-Online – pour les particuliers, professions libérales, artisans, TPE et PME...

- » Existence de solutions réseau – MainInBlack-PRO – pour les entreprises et les grands comptes. C'est une passerelle filtrant les messages entrants, en amont du serveur de messagerie. Cette passerelle est placée dans la DMZ de l'entreprise. L'administration est faite directement par par l'utilisateur final, après l'installation. MailInBlack-PRO ne nécessite aucune maintenance de la part de l'administrateur réseau : chaque utilisateur possède un espace dédié avec ses propres listes d'expéditeurs légitimes et reçoit quotidiennement un rapport individuel de ses e-mails stoppés. Le tissu économique européen, constitué en France de 99% d'entreprises de moins de 250 salariés (répartition proche dans les autres pays), est la cible privilégiée de MailInBlack-PRO.
- » Aucun dispositif n'est à installer côté client – aucun téléchargement – aucun code ne s'exécute
- » Utilisation d'un antivirus (BitDefender – classé N° 1 dans tous les critères de tests réalisés par le magazine L'Ordinateur Individuel de mai 2005).
- » WebMail pour les travailleurs nomades (en version on-line)
- » Indépendance totale de la société MailInBlack (hommes et capitaux)

MailInBlack fonctionne avec tous les clients de messagerie sans restriction dont votre client de messagerie actuel et vous n'avez aucune habitude à changer. Tous vos historiques de correspondances sont inchangés. Rien n'est installé. Rien n'est enlevé.



Figure 8 : Message d'authentification

10.10. Le principe général de MailInBlack

10.10.1. Première étape

Quelqu'un, disons Pierre Martin, vous écrit, tout à fait habituellement. C'est la première fois qu'il le fait depuis que vous avez installé MailInBlack. Votre boîte s'appelle Jean Dupont et le sujet du message qu'il vous envoie est, par exemple: "Invitation au vernissage de ma nouvelle expo".

10.10.2. Seconde étape

Vous ne recevez rien et vous ne faites rien. Le message est mis en file d'attente chez MailInBlack et l'expéditeur, Pierre Martin, reçoit immédiatement un message (ce sera la seule fois où il recevra ce message) dont le sujet, personnalisé, est : "Re: [Invitation au vernissage de ma nouvelle expo] vers Jean Dupont".

10.10.3. Troisième étape

Pierre Martin ouvre cette correspondance qui est le petit message très courtois suivant. Bien que ce soit MailInBlack, un robot, qui ait envoyé automatiquement ce message, tout est fait pour qu'il semble parvenir de vous-même. Ce petit message est d'ailleurs personnalisable dans le texte comme par l'adjonction d'une image (votre photo pour un particulier, le logo de votre entreprise pour un professionnel...).

10.10.4. Quatrième étape

Pierre Martin clique sur le lien pour s'identifier et est envoyé sur le serveur de MailInBlack. Il se trouve face au test de Turing. Si Pierre Martin est un robot d'expédition de spam, il ne pourra rien faire de ce test, seul un humain peut faire ce qui est demandé : recopier un mot de passe masqué et l'envoyer.

10.10.5. Fin

C'est fini. Pierre Martin vient de prouver son humanité et est définitivement identifié comme tel – il est mis en liste blanche. Un petit message de confirmation s'affiche.

MailInBlack est soutenu par l'Oséo-Anvar, Agence nationale de valorisation de la recherche, dite "Agence française de l'innovation".




Figure 9 : Vérification de l'expéditeur

11. Ressources

¹ Etude du Pew Internet & American Life Project du 10.04.05 

http://www.pewinternet.org/PPF/r/155/report_display.asp

² Viruses and spam will cause Net's collapse 

http://www.iol.co.za/index.php?set_id=1&click_id=31&art_id=qw1098104405860B215

³ Microsoft met KO le roi du spam !

<http://www.generation-nt.com/actualites/6538/Microsoft-met-KO-le-roi-du-spam>
<http://www.liberation.fr/page.php?Article=288943>

Neuf ans de prison pour avoir abusé du spam

[http://www.01net.com/editorial/255725/justice/\(mise-a-jour\)-neuf-ans-de-prison-pour-avoir-abuse-du-spam/](http://www.01net.com/editorial/255725/justice/(mise-a-jour)-neuf-ans-de-prison-pour-avoir-abuse-du-spam/)

⁴ Scott Richter – OptInRealBig

<http://www.spamhaus.org/rokso/listing.lasoz?op=cn&spammer=Scott%20Richter%20-%20OptInRealBig>

⁵ Rokso List – Liste des plus gros spammeurs au monde


<http://www.spamhaus.org/rokso/>

⁶ Origine du mot Spam


http://assiste.com/p/spam/spam_025_definition_2.php

⁷ FTC - Federal Trade Commission 

<http://www.ftc.gov/>

⁸ Etude FTC – 96% des spams sont des offres commerciales ou d'investissement mensongères 

<http://www.pcinpact.com/link.php?url=http%3A%2F%2Fwww.ftc.gov%2Freports%2Fspam%2F030429spamreport.pdf>

⁹ Preliminary Results Show 31% of Respondents Have Clicked on Embedded Links 

http://www.mirapoint.com/company/news_events/press/20050323.shtml

¹⁰ Méthode de diffusion « classique » des spam

http://assiste.com/p/spam/spam_023_chaine_du_spam.php

¹¹ Risque de complicité de prolifération virale et d'envoi de Spam

http://assiste.com/p/spam/spam_029_complice.php

¹² Virus

http://assiste.com/p/carnets_de_voyage/virus.php

¹³ W32.Mydoom est un ver d'envoi en masse de courrier électronique qui utilise son propre moteur SMTP pour envoyer du courrier électronique aux adresses récupérées dans le carnet d'adresses Windows de l'ordinateur infecté. Par exemple, la variante ax de ce ver :

<http://www.symantec.com/region/fr/techsup/avcenter/venc/data/fr-w32.beagle.u@mm.html>

<http://www.symantec.com/region/fr/techsup/avcenter/venc/data/fr-w32.mydoom.ax@mm.html>

¹⁴ PC Zombie : Définition d'un ordinateur Zombie – Réseau de Zombies

Un Zombi est un ordinateur dans lequel ont été implantées une ou plusieurs fonctions cachées qui le mettent sous le contrôle d'un intrus malveillant (pirate, hacker, maffieux du Net, spammeur...) sans que le propriétaire de l'ordinateur en ait conscience. Lorsque le malveillant contrôle plusieurs zombies (souvent des centaines de milliers) il les fait coopérer, se constituant ainsi, gratuitement, une formidable puissance de calcul. Lorsque c'est un spammeur qui contrôle un réseau de zombies, en un instant chaque zombi envoie

¹⁵ PC Zombie - Complice des spammeurs
http://assiste.com/p/spam/spam_029_complice.php

¹⁶ PC Zombie – Plusieurs exemples d'usage d'un réseau de PC à distance, légitime ou usurpé

http://assiste.com/p/internet_attaquants/iosdt_exe.php

¹⁷ Inconscience professionnelle - un informaticien aide son client à spammer
http://assiste.com/p/spam/spam_040_inconscience_1.php

¹⁸ Washington déclare l'infoguerre (Radio France International – 19.02.2003)
http://www.radiofranceinternationale.fr/actufr/articles/038/article_20083.asp

¹⁹ Invasion du spam raciste allemand
<http://www.01net.com/article/245091.html>

²⁰ Le virus Sober (W32/Sober-G) et le spam raciste allemand
<http://www.sophos.fr/pressoffice/pressrel/20040611soberg.html>
<http://www.vulnerabilite.com/communiqués/471>
<http://www.symantec.com/region/fr/techsup/avcenter/venc/data/pf/fr-trojan.ascetic.c.html>

²¹ Le spam politique – Attention, le communisme est de retour !

<http://www.generation-nt.com/actualites/5844/Le-spam-politique-debarque>

²² Le virus Bagle

<http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.gen.html>
<http://www.sophos.fr/virusinfo/analyses/w32baglebk.html>
<http://www.microsoft.com/france/securite/alertes/bagle.aspx>
<http://www.symantec.com/region/fr/techsup/avcenter/venc/data/fr-w32.beagle.u@mm.html>

²³ Sober.N

<http://securityresponse.symantec.com/avcenter/venc/data/w32.sober.n@mm.html>

²⁴ Sat Jun 26, 2004

85% will open an attachment, if it came

from a friend

85% of 1,162 people questioned by Tickbox.net and online marketing agency Marketiers4dc said they would open an attachment sent by a friend or colleague, compared to 84% last year. Humorous content was cited as the top reason people opened attachments or forwarded them to friends. 83% of respondents forwarded emails to make the recipient laugh. 58% sent emails on to recommend something.

<http://tickbox.net/index.php>

²⁵ Le virus PEBCAK

<http://assiste.com/p/virus/pebcak.php>

²⁶ Top Ten Sophos des virus - Avril 2005

<http://www.sophos.fr/pressoffice/pressrel/20050502topten.html>

²⁷ W32/Mytob-Z

<http://www.sophos.com/virusinfo/analyses/w32mytobz.html>

<http://www.sophos.fr/virusinfo/analyses/w32mytobz.html>

²⁸ Cheval de Troie

http://assiste.com/p/carnets_de_voyage/roians.php

²⁹ Backdoor – Porte dérobée

http://assiste.com/p/internet_attaques/backdoor.php

³⁰ Est-ce qu'un trojan est un virus ?

http://assiste.com/p/internet_attaques/trojan_virus.php

³¹ Définition d'un Trojan (Cheval de Troie)

http://assiste.com/p/internet_attaques/trojan_definition.php

http://assiste.com/p/carnets_de_voyage/roians.php

³² « Charge active » ou « Payload »

Terme emprunté au vocabulaire militaire où il désigne le composant actif d'un l'engin explosif. Sa nature, et plus encore sa masse, sont fonction de l'effet recherché. Dans un virus, c'est partie du code qui est affectée à la fonction du virus, par opposition aux autres parties du code affectées à sa réplication et à sa dissimulation.

³³ Serveur SMTP

Simple Mail Transfer Protocol. Dans un réseau TCP/IP (le réseau Internet, par exemple), le protocole SMTP permet de faire circuler des messages de serveurs de messagerie en serveur de messagerie, raison pour laquelle vous devez indiquer un serveur SMTP dans votre outil de messagerie pour envoyer des messages (et vous avez un mini serveur SMTP implanté dans votre Outlook Express, ThunderBird...). Les spammeurs implantent en cachette de véritables serveurs de messagerie furtifs sur les PC dont ils prennent le contrôle.

³⁴ Prise de contrôle à distance – outils commerciaux (normalement utilisés « légitimement »)

http://solutions.journaldunet.com/0309/030918_accesdistants.shtml

³⁵ 30.000 PC « zombies » pris en otages chaque jour à des fins de spam ou d'arnaque

<http://www.lexpansion.com/compteur/compteur.asp?compteurid=689&redirUrl=http://www.lexpansion.com/art/2563.78366.0.html>

³⁶ 30 % du spam émis dans le monde provient de PC zombifiés

<http://www.sophos.fr/pressoffice/pressrel/20040228dirtydozen.html>

³⁷ 50 % du spam émis dans le monde provient de PC zombifiés

<http://www.sophos.fr/pressoffice/pressrel/20050411dirtydozen.html>

³⁸ Keylogger

http://assiste.com/p/internet_attaques/keylogger.php

³⁹ Le London Action Plan on Spam Enforcement Collaboration

http://www.ftc.gov/os/2004/10/041012lon_donactionplan.pdf

<http://www.ftc.gov/opa/2004/10/spamconference.htm>

<http://www.vircom.com/News/press2005-03-21.asp>

⁴⁰ Phishing

http://assiste.com/p/internet_attaques/phishing.php

⁴¹ Hoax

http://assiste.com/p/internet_attaques/hoax.php

⁴² La Joe Job Attack

http://assiste.com/p/spam/joe_job_attack.php

⁴³ Nigerian spam

http://assiste.com/p/internet_attaques/nigerian_spam.php

⁴⁴ Alan Ralsky – 3 milliard de spam par jour

http://www.freep.com/money/tech/mwened22_20021122.htm

⁴⁵ Alan Ralsky – le revenu du spam ré-investi dans la pierre

<http://slashdot.org/comments.pl?sid=45801&threshold=0&commentsort=0&tid=111&mode=thread&pid=4735771#4735937>

⁴⁶ 7,5 millions de dollars pour un spyware

http://www.reseaux-telecoms.com/cso_btrees/05_06_17_14474_5_697/CSO/Newsco_view

⁴⁷ Coût du spam en 2003 – estimé à 20 milliards de dollars

<http://www.lexpansion.com/art/2264.7261.7.0.html>

⁴⁸ Coût du spam – doublement chaque année

<http://www.lexpansion.com/art/2465.7637.6.0.html>

⁴⁹ L'article de 2003 du Nucleus Research : Spam: The Silent ROI Killer

La consultation des autres articles du Nucleus Research est payante dont la

mise à jour 2004 de cet article

<http://www.nucleusresearch.com/research/d59.pdf>

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

⁵⁰ Taking out the garbage of spam

<http://www.scmagazine.com/features/index.cfm?fuseaction=featureDetails&newsUID=4d9cd7e7-f3e6-49d1-a311-6951ff1077f9>

⁵¹ The High, Really High Or Incredibly High Cost Of Spam

<http://www.lexisone.com/balancing/article/s/n080003d.html>

⁵² The CAN-SPAM Act

<http://www.ftc.gov/bcp/online/pubs/buspubs/canspam.htm>

<http://www.can-spam-act.com/>

⁵³ FTC - Federal Trade Commission

<http://www.ftc.gov/>

⁵⁴ DGCCRF - Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes

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

⁵⁵ Position de la CNIL sur la prospection par courrier électronique dans le cadre professionnel

<http://www.cnil.fr/index.php?id=1780>

⁵⁶ Tracking et profiling

Espionnage consistant à tracer la navigation d'un internaute pour en dégager son profil, essentiellement de consommateur. En matière de correspondance électronique, la technologie utilisée est le Web-Bug, quelque-fois sous des formes subtiles

Web-Bug

http://assiste.com/p/internet_attaques/web_bug.php

Did They Read It – Le Web-Bug commercial du courrier électronique

http://assiste.com/p/internet_attaques/didtheyreadit_did_they_read_it.php

⁵⁷ Spywares

http://assiste.com/p/internet_attaques/spyware.php

⁵⁸ Les dispositions légales anti-spam : inefficaces et contre-productives !

http://www.domaines.info/chronique.php?chronique_id=50&z=100

⁵⁹ Ubuesque : près de 4 millions de dollars de dommages et intérêts pour refus d'être spammé.

http://www.reseaux-telecoms.com/cso_btrees/05_03_18_17012_1_776/CSO/Newsco_view

⁶⁰ Spam - Brontosaure contre Turing

http://assiste.com/p/spam/spam_044_brontosaures_turing.php

⁶¹ Les filtres anti-spam : 10 à 20 % de dommages collatéraux !

<http://www.journaldunet.com/0504/050420spam.shtml>

⁶² Page, sur le site SpamCop, permettant de dénoncer un spam :

<http://www.spamcop.net/anonsignup.shtml>

⁶³ Chiffres clé, hashcodes, MD5

http://assiste.com/p/internet_utilitaires/suimmerproperties.php

⁶⁴ One company arms both sides in spam war

<http://www.coax.nl/news/2003/dec/cnet.html>

http://msn-cnet.com.com/2100-1032_3-5111556.html

<http://www.bearcave.com/links.htm>

<http://www.computercops.biz/postp37622.html>

⁶⁵ AOL now filtering based on whether they like embedded URLs

<http://catless.ncl.ac.uk/Risks/23.09.html#subj5>

⁶⁶ Echec des filtres à règles

http://assiste.com/p/spam/camouflage_de_spam_1.php

⁶⁷ Echec des analyses de corps

http://assiste.com/p/spam/ascii_art.php

⁶⁸ Echec des filtres bayésiens

http://assiste.com/p/spam/camouflage_de_spam_3.php

⁶⁹ Reverse Mail Exchanger (RMX)

<http://www.ietf.org/internet-drafts/draft-danisch-dns-rr-smtp-04.txt>

⁷⁰ Sender Permitted From (SPF)

<http://spf.pobox.com/>

⁷¹ Designated Mailers Protocol (DMP)

<http://www.pan-am.ca/dmp/>

⁷² Yahoo! Domain Keys

<http://antispam.yahoo.com/domainkeys>

⁷³ Microsoft Caller ID for Email

http://www.microsoft.com/mscorp/twc/privacy/spam_callerid.msp

⁷⁴ Faille - GFI MailSecurity efface tous les messages de tous ses clients

<http://www.generation-nt.com/actualites/6030/Filtres-a-Spam-faillibles>

⁷⁵ Mises à jour automatiques

http://assiste.com/p/internet_attaques/mises_a_jour_automatiques.php

⁷⁶ Les contrôles anti-spam font manquer des échéances à plus d'un tiers des salariés

http://www.mag-secur.com/article.php3?id_article=2354

⁷⁷ Des alertes ouragans filtrées par l'antispam d'AOL...

<http://fr.news.yahoo.com/050503/308/4e65c.html>


⁷⁸ Verizon's Anti-Spam Results in Collateral Damage

<http://www.spambutcher.com/misc/44.html>

⁷⁹ Verizon sued over spam filtering - Verizon faces lawsuit over email blocking

<http://arstechnica.com/news.ars/post/20050122-4546.html>


http://www.theregister.co.uk/2005/01/21/verizon_class_action/

⁸⁰ Barracuda - Faq 

http://www.barracudanetworks.com/ns/suport/spam_firewall_faq.php

⁸¹ Barracuda – Livre blanc sur les messages non délivrés 

http://www.barracudanetworks.com/ns/downloads/barracuda_NDR_whitepaper.pdf

⁸² Barracuda – Faux positifs et faux négatifs 

<http://www.networkworld.com/reviews/2004/122004spamside3.html>

⁸³ CipherTrust – Essayer de diminuer le taux de faux positifs

http://www.ciphertrust.com/resources/articles/articles/false_positives.php

⁸⁴ Cloudmark's SpamNet – Prétention au zéro faux positifs !

<http://www.cloudmark.com/press/releases/?release=2004-07-29>

⁸⁵ Cloudmark's SpamNet – 14% de faux positifs

<http://www.networkworld.com/reviews/2003/0915spam.html>

⁸⁶ Cloudmark's SpamNet – Faux positifs et faux négatifs

<http://yahoo.pcworld.com/yahoo/article/0,aid,115885,00.asp>

⁸⁷ Ipswitch intègre la technologie anti spam de Mail-Filters.com

<http://www.publi-news.fr/data/14042005/14042005-092055.html>

⁸⁸ SpamCure

...The result is a unique combination of spam detection techniques that is seldom fooled by spammers' tricks and consistently catches 95% of the spam with less than 1 false positive in 1,000,000 messages...

<http://www.mail-filters.com/Products/SpamCure.htm>

⁸⁹ La nouvelle fonctionnalité SURBL de GFI MailEssentials 11


http://www.gfsfrance.com/news/fr/mes111_aunch.htm

⁹⁰ Symantec Mail Security 8200

<http://www.symantec.com/region/fr/press/n050424.html>

⁹¹ BlackSpider Lance MailControl En France

http://www.blackspider.com/news_and_resources/press_releases/12Oct04-BlackSpider_lance_MailControl_en_France-FR.pdf

⁹² Mail-Filters 

http://mail-filters.com/Products/products_main.htm

⁹³ Documentation DPL – Dolphian

http://www.dolphian.com/anti_spam.php
http://www.dolphian.com/pdf/doc_dmp_fr.pdf

⁹⁴ Gmail spam filter effectiveness 

http://www.spamfo.co.uk/index.php?option=com_content&task=view&id=000291

⁹⁵ Sender ID – Microsoft

<http://www.microsoft.com/mscorp/safety/technologies/senderid/default.aspx>

⁹⁶ L'IETF refuse d'entériner la technologie anti-pourriel Sender ID de Microsoft

<http://www.pourriel.ca/archives/000927.php>

⁹⁷ La fondation Apache rejette le projet Sender ID

<http://www.zdnet.fr/actualites/telecoms/0,39040748,39170251,00.htm>

⁹⁸ Spam-aware – taux de faux positifs et de faux négatifs

<http://www.spam-aware.fr/index.php?page=discover#part2>

⁹⁹ Vade Retro

http://www.antispam.fr/index_part.asp

¹⁰⁰ Free.fr et son "service" anti-spam

<http://mfilter.free.fr/>

¹⁰¹ "Well trained" filter can determine up to 99.5% of spam emails

<http://www.glocksoft.com/sc/index.htm>

¹⁰² Alan Turing WebSite - Un site entièrement consacré à Alan Turing

<http://www.turing.org.uk/>

¹⁰³ Tests de Turing – historique

http://assiste.com/p/spam/spam_043_tests_de_turing.php

¹⁰⁴ IBM FairUCE reconnaît l'ultime efficacité des Tests de Turing

<http://www.alphaworks.ibm.com/tech/fairuce>

¹⁰⁵ SPF - Sender Policy Framework 

<http://spf.pobox.com/>

¹⁰⁶ SPF - Sender Policy Framework

<http://www.01net.com/article/251647.html>

¹⁰⁷ Les antivirus « classiques » ou « ordinaires », à bases de signatures, blacklists, sandbox...

http://assiste.com/p/familles/antivirus_commerciaux.php

¹⁰⁸ Les anti-spywares « classiques » ou « ordinaires », à bases de signatures, blacklists, sandbox...

http://assiste.com/p/familles/anti_spywares.php

¹⁰⁹ Contrôle d'intégrité et contrôleurs d'intégrité

http://assiste.com/p/familles/controle_integrite.php

¹¹⁰ Trojans

http://assiste.com/p/carnets_de_voyage/trojans.php

¹¹¹ Spywares

http://assiste.com/p/carnets_de_voyage/spywares.php

¹¹² Spam Arrest est un spammeur !

http://assiste.com/p/internet_utilitaires/spam_arrest.php