Etat de l'art du spam, solutions et recommandations

Travail de diplôme réalisé en vue de l'obtention du diplôme HES

par :

Philippe GUILLON

Conseiller au travail de diplôme :

Rolf HAURI, Chargé d'enseignement HES

Genève, le 10 décembre 2008

Haute École de Gestion de Genève (HEG-GE)

Filière informatique de gestion

Déclaration

Ce travail de diplôme est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre de bachelor en informatique de gestion. L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de diplôme, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de diplôme, du juré et de la HEG.

« J'atteste avoir réalisé seul le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Genève, le 10 décembre 2008

Philippe Guillon

Remerciements

Je remercie tout d’abord M. Rolf Hauri pour sa disponibilité et ses précieux conseils tout au long de ce travail.

Merci également à M. Enrico Vigano pour m’avoir donné l’idée de traiter du sujet des spams, ainsi que de m’avoir mis en contact avec Paléo.

Enfin, je remercie M. Etienne Cuellar (Paléo) pour avoir accepté de répondre à mes questions. Sa participation m’a ainsi permis de comprendre la situation de Paléo en matière de gestion du spam.

Sommaire

Célèbre pour les nombreux désagréments qu'il cause, le spam est devenu en l'espace d'une dizaine d'années le principal fléau d'internet. Agissant à l'échelle mondiale, le nombre de victimes est colossal. Malgré l'ampleur du préjudice causé, force est de constater que la situation n'est toujours pas maîtrisée.

Dans un premier temps, l'objectif de ce travail est donc de dresser un état de l'art du spam. Ceci nous a permis de connaître ses origines, ses objectifs et la façon dont il a évolué, ainsi que les démarches plus ou moins réussies entreprises pour le contrer. Cette étude nous a aidés d'une part à comprendre la situation dans laquelle nous nous trouvons actuellement et d'autre part de prévoir autant que possible l'évolution future du spam.

Dans un deuxième temps, l'aspect pratique de la lutte anti-spam a été abordé. L'objectif est de fournir un ensemble d'informations et de recommandations afin d'aider tout responsable informatique à choisir une solution anti-spam adaptée à son cas. Une succession d'étapes permettant de mener à bien un tel projet est aussi proposée et servira, si besoin est, de fil rouge.

Pour terminer, une étude de cas présente de façon résumée la situation rencontrée par l'association Paléo par rapport à sa gestion des spams.

Table des matières

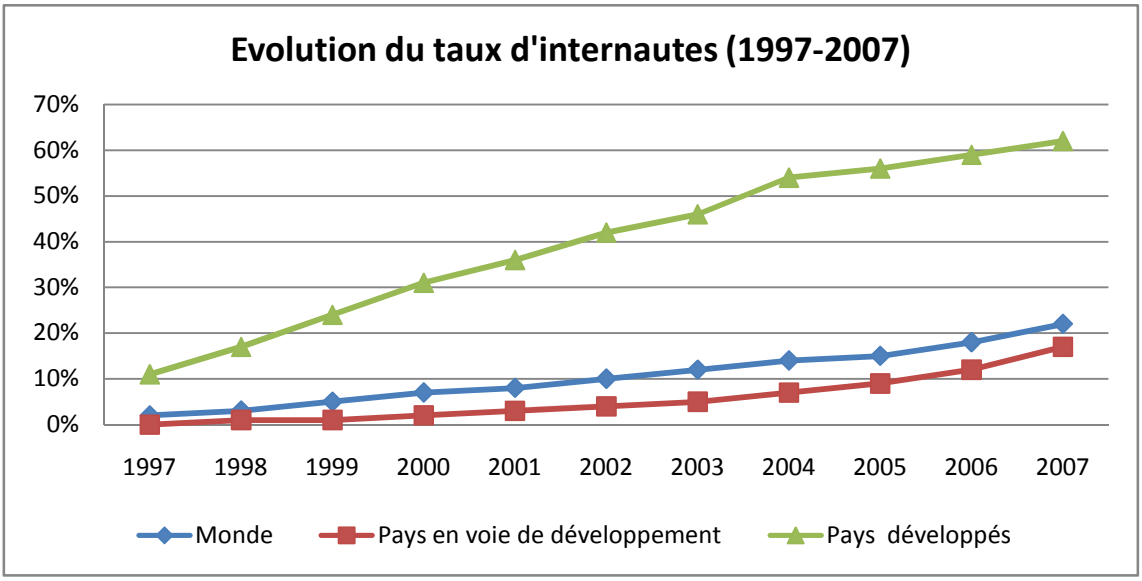
Liste des Tableaux

Liste des Figures

Introduction

Les moyens de communication modernes ont connu cette dernière décennie une expansion massive. Les entreprises voient dans ces nouveaux outils la possibilité d'améliorer de façon significative leur efficacité en communiquant toujours plus vite, de façon plus efficace et à des coûts toujours plus faibles. Selon l'Insee, 97% des entreprises disposaient d'un accès internet en 2007, contre 82% en 2003 [INS].

L'accessibilité facilitée à internet et à l'informatique de façon générale a aussi permis aux particuliers (presque indépendamment de leurs moyens financiers) de recourir massivement à ces nouveaux services devenus courants et très utilisés au quotidien. Cet engouement est certainement loin d'être terminé, en regard du prix de l'électronique toujours plus abordable, des connexions haut-débit accessibles à la majorité, aux outils informatiques plus conviviaux et faciles d'utilisation ainsi qu'aux utilisations du web toujours plus variées et ludiques (réseaux sociaux, blogging, jeux online, VoD, etc.).



Source : International Telecommunication Union [ITU]

Rester connecté et joignable en tout temps devient aussi toujours plus courant. Il n'est par exemple pas rare d'accéder à sa messagerie professionnelle hors des heures de travail. Cela est valable aussi lorsque l'on n'est pas chez soi, grâce à de nouvelles technologies : WiFi disponible massivement dans les lieux publics ou à l'hôtel (gratuitement ou à des tarifs dérisoires), forfaits data (parfois illimités) utilisant les réseaux UMTS ou EDGE, système push-mail, etc.

Parallèlement à cette frénésie s'est développé un véritable fléau : le spam.

Notons également que le spam est parfois appelé « pourriel », « polluriel », « courrier indésirable », voir « junk mail ».

Il peut rendre inefficace l'utilisation de la messagerie au sein d'une entreprise, alors que celle-ci est un outil incontournable qui permet d'assurer les communications aussi bien en interne qu'avec l'extérieur. Nous verrons qu'il véhicule aussi d'autres menaces. Pour ces raisons, se protéger du spam est devenu indispensable.

Il existe de nombreuses définitions du spam, qui se ressemblent plus ou moins. Selon la CNIL, le spam est défini de la façon suivante :

> *« Le "spamming" ou "spam" est l'envoi massif, et parfois répété, de courriers électroniques non sollicités, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière. »* *[CNIL01]*

Cette affirmation caractérise bien le phénomène, mais on peut tout de même la nuancer : auparavant cantonné aux courriers électroniques, le spam use aujourd'hui d'autres canaux de diffusion tels que les forums, les blogs (par l'entremise des commentaires), voir certains services de messagerie instantanée.

Le spam est parfois décrit de façon moins restrictive. C'est par exemple le cas de la définition suivante publiée en 1997 par Eric Demeester sur son site personnel :

> *« Message dont le mode de diffusion et/ou le contenu sont nuisibles pour les réseaux et/ou pour les lecteurs »* *[HAS01]*

Rien n'est donc précisé quant à la quantité, à la fréquence, au rapport expéditeur / destinataire ou encore au moyen de collecte de l'adresse électronique.

Ces deux définitions illustrent bien qu'il s'agit d'une différence de perception. La première conviendra habituellement à un éditeur anti-spam ou dans une plus large mesure à toute personne « initiée » au phénomène, tandis que la deuxième correspondra d'avantage à la plupart des utilisateurs. Il n'est par exemple par rare de voir que les membres participants à des forums désignent comme spam tous les topics créés à des fins publicitaires, même s'ils proviennent d'un webmaster postant un lien vers son site personnel, de façon manuelle et donc en faible quantité.

1. Etat de l'art du spam

Comme détaillé ci-après, le spam n'est pas un phénomène nouveau, mais nous verrons qu'il a su évoluer avec son temps. Ces évolutions, induites couramment par les spammeurs et les acteurs de la lutte anti-spam touchent de nombreux aspects du domaine. Ce chapitre a donc pour objectif d'expliquer comment tout à commencé, de faire le point sur la nature de ces évolutions puis d'envisager l'avenir du spam.

1.1 Naissance et débuts du spam

1.1.1 Origine du mot « spam »

A l'origine, le mot a été inventé en 1937 par le gagnant d'un concours organisé par la société américaine Hormel Foods, le but étant de tenter de gagner 100$ en trouvant un nom pour leur nouveau produit : du jambon épicé. « SPAM » fut donc la marque retenue, mot formé à partir de « SPiced hAM » [LNX01] [AKS].

Cette préparation, souvent synonyme de mauvaise nourriture (et utilisée par l'armée américaine durant la seconde guerre mondiale), est mise en scène dans un épisode de la série télévisée des années 70 « Monty Python's Flying Circus ». Dans cet épisode, les personnages empêchent toute discussion en scandant bruyamment « spam spam spam spam… ». Tout semble indiquer que la connotation informatique vient de là.

La société mère, insatisfaite de voir le nom de sa marque réutilisée par des éditeurs de solutions contre les messages indésirables a tenté plusieurs actions en justice sans succès [01N01].

1.1.2 Premier envoi massif

Contrairement à ce qu'on pourrait penser, le premier spam est plus âgé qu'internet [LNX03]. En effet, il a été émis sur le réseau ARPANET (Advanced Research Projects Agency Network, prédécesseur d'internet et premier réseau à transfert de paquets [ARPA]). A l'époque, Gary Thuerk, spécialiste marketing chez DEC (Digital Equipment Corporation) a pensé bon d'émettre un message publicitaire vantant les mérites des nouveaux DECSYSTEM-2060T et 2020T supportant nativement le protocole ARPANET (sans être conscient des désagréments possibles qu'il pouvait causer).

Suite à une mauvaise utilisation de la messagerie, G. Thuerk se rend compte qu'une partie des destinataires n'ont pas reçu le courrier. Il procède donc à de nouveaux envois successifs. Au final, 393 personnes auraient reçu le message [ARO].

Les réactions sont vives. La DCA (Defense Communications Agency) gérant le réseau contacte immédiatement le patron de G. Thuerk pour lui faire part de son mécontentement. Une majorité des utilisateurs se plaignent également de ce message, à l'exception du célèbre Richard Stallman (défenseur du logiciel libre, créateur de la Free Software Foundation et de GNU) disant qu'il n'avait pas reçu ce message, mais que dans le cas contraire cela ne l'aurait pas dérangé. Il dit aussi que l'annonce de DEC est plus intéressante que les tonnes de courriers inintéressants qu'il reçoit tels que les messages annonçant des naissances.

1.1.3 Utilisations abusives à fins non commerciales

Quelques cas isolés d'utilisations inadéquates de systèmes de messagerie ont été constatées dans les années 80 et jusqu'au début des années 90. Ainsi, une annonce pour la vente d'un service de table est postée en 1985 sur un groupe de discussion usenet.

A cette époque, les participants aux (rares) systèmes de chat commencent à utiliser le terme « spam » pour définir les messages nuisibles envoyés massivement.

Plus tard en 1993, Richard Depew travaille sur le projet ARMM (Automated Retroactive Minimal Moderation), un système censé protéger les groupes de discussion usenet d'utilisations abusives. Malheureusement, dans le cadre d'un essai d'une version buggée d'ARMM, R. Depew envoie 200 messages sur le groupe news.admin.policy. Face aux récriminations, il s'excuse et utilise le mot « spam » pour désigner ses messages.

Le premier spam à l'échelle mondiale fut envoyé en janvier 1994 sur tous les groupes de discussion usenet : Un administrateur système de l'Université Andrews annonce la venue prochaine de Jésus (l'histoire ne dit pas s'il a conservé son travail !).

1.1.4 Utilisations abusives à fins commerciales

Le premier spam lancé à des fins strictement commerciales fut celui du cabinet Canter & Siegel en mars 1994 [AKS]. Laurence Canter inonda les groupes de discussion usenet au moyen d'un script Perl. Le message vantait les services du cabinet en matière d'obtention d'une Green Card (carte de travail étatsunienne). Le message aurait été posté sur près de 6'000 groupes de discussion pour un total de 12Mo, ce qui représentait à l'époque environ 10% du trafic quotidien sur usenet [AMAC]. En retour, les vives critiques des internautes ont rapidement submergé les installations du cabinet (téléphones, faxs, emails).

Cette affaire marqua un véritable tournant dans l'évolution du spam. Contrairement aux utilisations plus marginales rencontrées dans le passé, de nombreuses entreprises peu scrupuleuses prendront peu à peu conscience de la puissance « médiatique » offerte par le spamming. C'est ainsi que la pratique se démocratisa, de même que l'utilisation courante du terme « spam ».

1.2 Evolution du spam

1.2.1 Provenance

Auparavant émis majoritairement depuis les Etats-Unis, les spécialistes constatent dans les années 2000 que le spam provenant de Chine augmente.

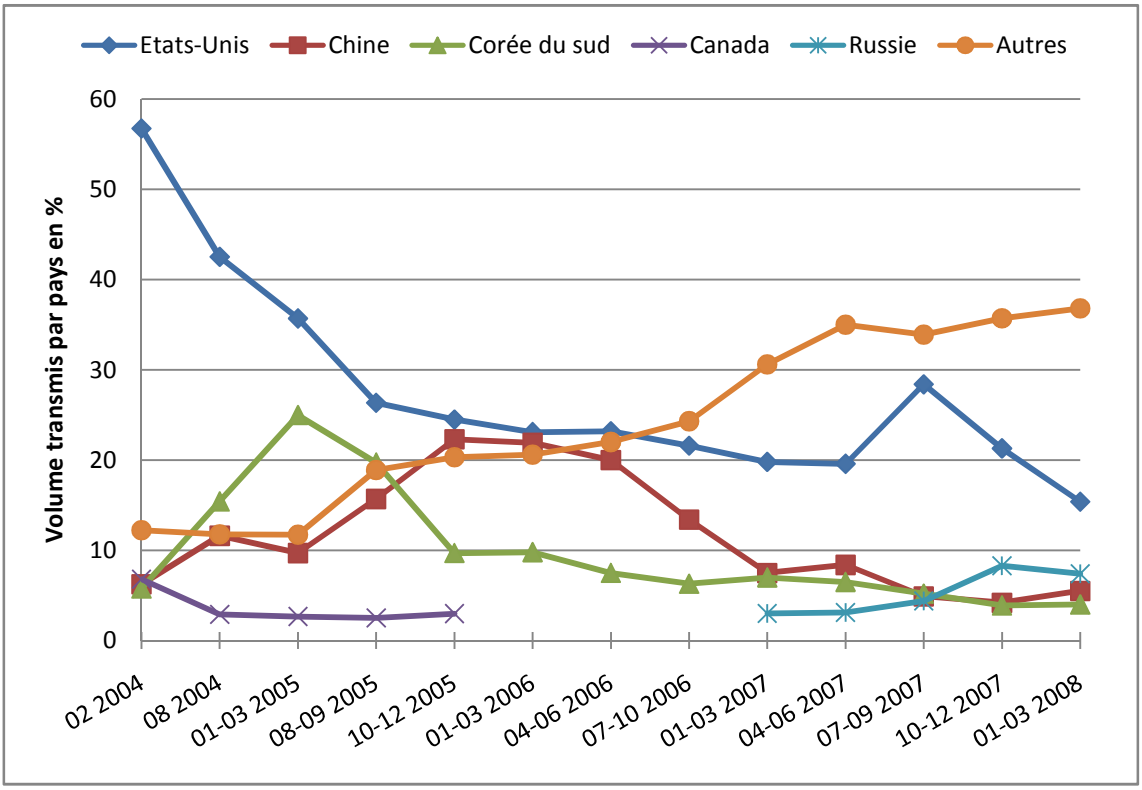
En effet, on constate à cette époque un accroissement effréné du nombre de Chinois connectés à internet. De 2000 à 2008, ce nombre a augmenté de 833% grâce aux dispositions prises par le gouvernement : augmentation des salaires et baisse du prix du matériel informatique. On estime à ce jour que 250 millions de Chinois surfent sur internet, soit 30 millions de plus que les étatsuniens. Avec seulement 16% de la population chinoise raccordée à internet contre 71% pour les étatsuniens, les possibilités d'expansion dans le futur sont considérables [FR24].

Cet accroissement conduit naturellement à une augmentation du nombre d'équipements en service. Certains serveurs mal entretenus deviennent des relais à spams. Il semblerait qu'à l'époque, les ISP chinois n'étaient pas soumis aux mêmes pressions politiques que leurs homologues américains et étaient moins disposés à prendre suffisamment de mesures contre le spam. Nick Nicholas, chef de MAPS, une association californienne à but non lucratif aidant les ISP à lutter contre le spam, précise que les Chinois n'avaient pas encore suffisamment pris conscience de l'importance du problème. De ce fait, les administrateurs avaient tendance à utiliser des versions trop anciennes de leurs logiciels, causant des failles de sécurité exploitables par les spammeurs du monde entier. L'ampleur est telle que de nombreux prestataires de services chinois ont été blacklistés. Certains petits ISP en sont même venus à bannir tout ce qui provenait du pool d'adresses de China Telecom, entreprise détenue majoritairement par le gouvernement et assurant les liaisons de backbone pour une grande quantité de prestataires de services du pays [CNN].

D'après les rapports réalisés par Sophos [SOPH01] (éditeur de solutions anti-spam), 56.7% des spams émis en février 2004 dans le monde proviennent des Etats-Unis. Il s'agit de loin du pays le plus touché, puisque la deuxième place du classement est

occupée par le Canada avec seulement 6.8% du volume mondial (8 fois moins !). Viennent ensuite la Chine et la Corée du sud avec respectivement 6.2% et 5.8%.

Il convient de relativiser ces statistiques désignant la provenance d'un spam, puisque les messages expédiés depuis des ordinateurs infectés par des vers et backdoors empêchent généralement de retracer l'origine réelle du spam. Pour éviter toute confusion, il s'agit donc des pays les plus grands relayeurs. C'est la raison pour laquelle certains pays ne figurent pas sur la liste des 12 plus grands émetteurs de spam. A ce sujet, les spammeurs de Russie utiliseraient selon Sophos couramment cette technique virale et seraient à l'origine d'une grande quantité de spams (environ 30%), bien que le pays figure seulement à la 28ème place du classement pour 2004.



Le graphique ci-dessus créé sur la base des rapports trimestriels de Sophos de 2004 à 2008 présente l'évolution des plus grands relayeurs de spam (pour des raisons de lisibilité, nous n'avons gardé que les pays les plus significatifs). Le tracé orange (« Autres ») représente le volume de tous les pays classés après la 12ème position (à savoir le total cumulé des plus petits relayeurs de spams).

Première constatation : Les Etats-Unis étaient et sont toujours les plus touchés par l'envoi de spams à partir de leurs équipements, malgré une amélioration notable : en l'espace de 4 ans, ils sont passés d'un volume relayé de 56.7% à 15.4%, soit environ 3.5 fois moins.

Cette réduction s'est répercutée dans un premier temps sur certains pays asiatiques : La Corée du Sud passe de 5.8% à 25% en l'espace d'un an environ (février 2004 à mars 2005), puis baisse fortement pour atteindre 9.7% à fin 2005, au « profit » de la Chine qui enregistre une évolution tout à fait inverse (9.7% en mars 2005 à 22.3% fin 2005).

Alors que le taux relayé par l'Asie fin 2006 est relativement modéré (Chine à 13.4% et Corée du Sud responsable de seulement 6.3%), la provenance du spam se diversifie : la quantité relayée par les pays les moins touchés (nommés « Autres » sur le graphique, ceux dont le taux les classe après les 12 plus grands relayeurs) devient toujours plus élevée. Fin 2006, ils s'élèvent à 24.3%. Début 2008, ils constituent 36.8% des spams émis dans le monde, tandis que les Etats-Unis ne comptent plus que pour 15.4%.

Plusieurs raisons peuvent expliquer la provenance toujours plus variée du spam. D'une part, il existe moins de pays refuges pour les spammeurs qu'autrefois, grâce à la prise de conscience générale conduisant à des mesures tant sur le plan technique (équipements mieux administrés et à jour) que juridique. D'autre part, on peut conclure que les spammeurs sont peu sélectifs quant à l'origine des moyens techniques exploités pour répandre du spam. Compte tenu qu'il existe des serveurs vulnérables dans toutes les régions du globe, ils sont tous sujets à servir tôt ou tard la cause des spammeurs. De plus, les attaques virales permettant la constitution de botnets (réseaux d'ordinateurs « zombies ») ont pour objectif de contaminer un nombre maximum d'ordinateurs, quel que soit leur provenance. En effet, bien qu'il soit plus intéressant de contaminer un ordinateur équipé d'une connexion large bande plutôt qu'un autre raccordé à une vieille liaison commutée, c'est avant tout le nombre d'équipements contrôlés qui prime (c'est d'ailleurs sur cette quantité qu'est fixé le tarif de location d'un botnet).

Apparue pour la première fois dans la liste des 12 pays les plus relayeurs de spam en mars 2007, la Russie occupe début 2008 la deuxième place (7.4% des spams mondiaux). Le Canada classé à la même position 4 ans plus tôt est par contre sorti du classement Sophos début 2006.

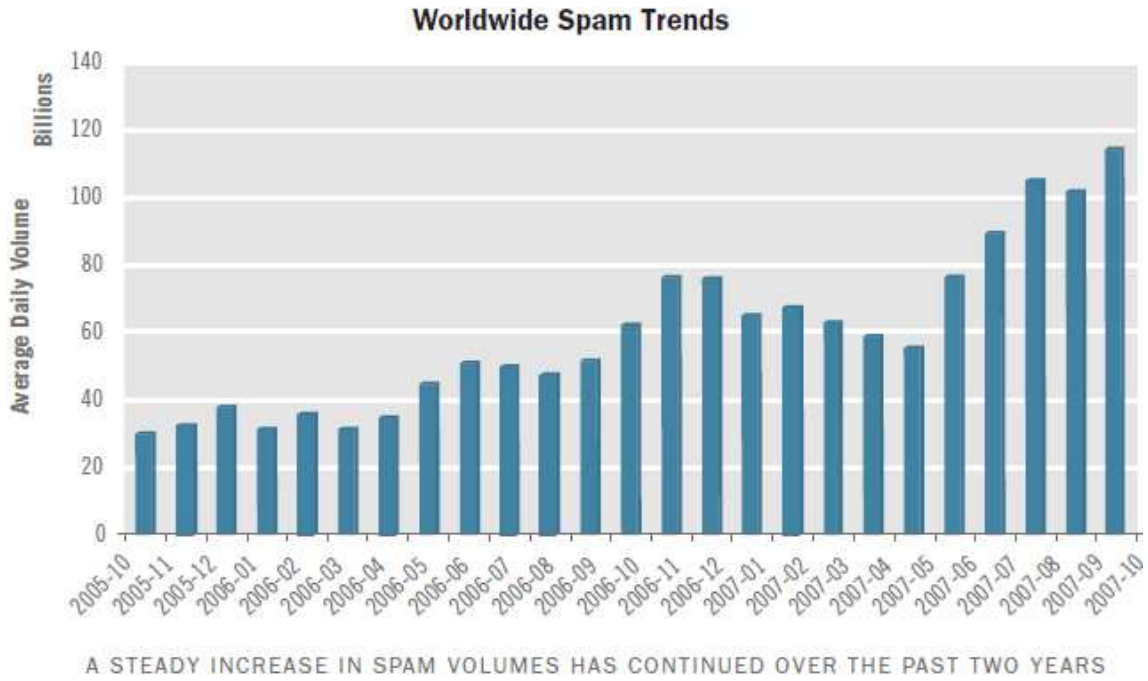
1.2.2 Volume

Malgré le faible taux de réponse mais grâce à son coût minime, l'envoi de spams en quantités démesurées garantit aux spammeurs une profitabilité accrue. Augmenter ces

volumes leur permet aussi de combler le « manque à gagner » causé par les solutions contre le spam désormais plus abouties.

Concrètement, les serveurs mal administrés (appelés « open relays ») sont moins nombreux que par le passé, mais ils ont été substitués par la création de botnets particulièrement efficaces (grande quantité de machines et connexions haut-débit courantes).

IronPort (filiale de Cisco Systems spécialisée dans la sécurité du courrier électronique) présente dans son rapport 2008 [IRON] une estimation du volume journalier de spams au cours des 2 dernières années :



Sans surprise, on constate que la tendance est à la hausse. En 2008, cela se confirme puisque le volume estimé en août s'élèverait à 150 milliards de spams par jour.

Le taux occupé par le spam par rapport au volume total des messages transmis varie selon les études et la période sur laquelle porte l'analyse. Il est chiffré à 80% d'après certains spécialistes, d'autres allant jusqu'à annoncer un taux record de 97% du volume total.

1.2.3 Contenus véhiculés et objectifs

Déterminer l'évolution précise des contenus véhiculés au cours du temps n'est pas chose aisée pour plusieurs raisons :

- Les contenus varient fortement plusieurs fois par année, parfois de façon contradictoire. Effectivement, il n'est pas rare de constater qu'un

type de message atteint un pic pendant quelques mois, rattrapé quelques temps plus tard par un autre, au gré des spammeurs qui changent de registre au fur et à mesure des opportunités qui s'offrent à eux suivant l'actualité (nouveaux médicaments, situation économique, etc.) ou des tendances actuelles de consommation.

- Les contenus sont très différents en fonction de la langue, mais aussi de la cible (particuliers ou entreprises). Une étude de la Cnil en 2002 illustre bien cela. Malheureusement, la quasi-totalité des statistiques publiées sont plus générales et ne tiennent pas compte de ce paramètre.
- Les honeypots utilisés par les différentes sociétés ou organismes ne sont pas tous spammés de façon identique (rien ne leur garantit qu'ils détiennent un échantillon hétérogène des types de spams émis partout dans le monde). A ce sujet, la comparaison d'études d'origines diverses réalisées à la même période ont révélé des différences notables.
- Les données produites par les diverses sources ne sont pas toutes consolidées de la même façon, ce qui rend leur comparaison problématique voir même hasardeuse.
- Les messages sont catégorisés de façon automatique, ce qui peut conduire à des inexactitudes plus ou moins marquées. Il est fréquent de voir qu'une partie des messages appartiennent à une catégorie générale « Produits » dans laquelle se retrouvent de nombreux messages promotionnels, alors que d'autres messages promotionnels sont triés plus précisément dans d'autres catégories. De plus, les messages déguisés en annonces promotionnelles visent parfois un tout autre but (fraude, propagation de malware, etc.). Ils ne sont donc pas toujours classés dans la bonne catégorie.
- Les analyses sont peu suivies. Une même source produisant des informations comparables fournit rarement des chiffres sur le long terme. Pire, le rachat d'entreprises rend l'exploitation des archives très difficile, c'est notamment le cas de l'entreprise Postini rachetée par Google en 2007, ou encore de Brightmail par Symantec en 2004.

Pour ces raisons, nous ferons preuve d'une certaine prudence quant à l'interprétation de ces résultats.

En dépit d'une gradation continue au cours des 10 dernières années, l'usage premier du spam reste le même : promouvoir la vente de produits ou services divers. Les domaines les plus concernés au premier semestre 2008 sont :

- la santé (vente de médicaments, soins divers, …)
- l'informatique, internet (logiciels, warez, hébergement, webdesign, …)
- la finance (crédits, investissements, …)

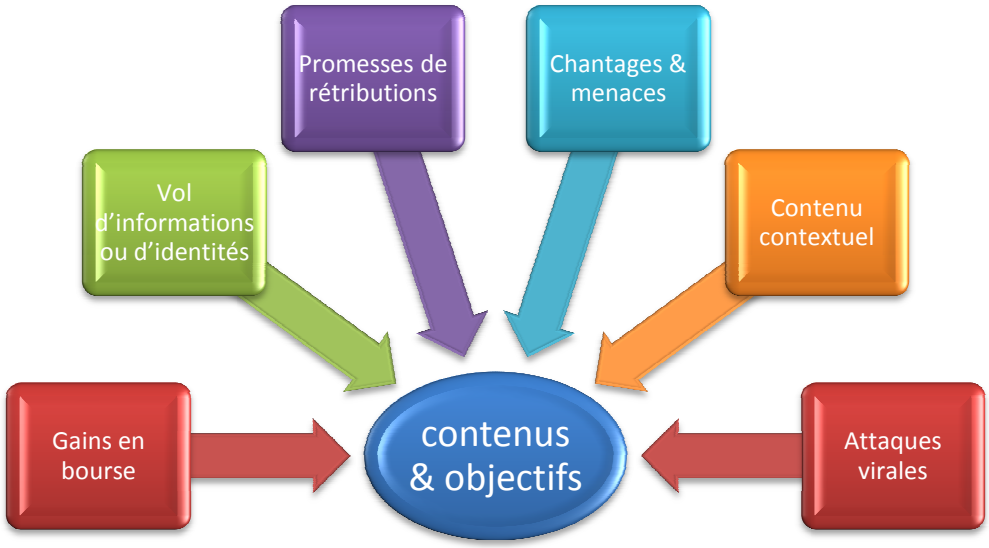
Cependant, la promotion de biens ou services n'est plus le seul objectif des spammeurs. Ils ont désormais recours à d'autres méthodes bien plus répréhensibles. Ces orientations ne sont pas nouvelles, mais nous constatons qu'elles sont toujours plus marquées mais aussi plus subtiles et mieux rôdées qu'auparavant. Citons par exemple l'explosion du spam boursier entre 2005 et 2006, l'augmentation des revenus

issus du phishing en 2007 par rapport à l'année précédente (meilleur taux de réponse rendu possible grâce à une mise en œuvre plus crédible), l'apparition de moyens de pression variés voir innovants (menaces, rançons), etc.

Les spammeurs ont recours à ces méthodes alternatives afin d'atteindre de nouveaux objectifs, tel que :

- satisfaire des besoins différents (par exemple voler des données, gagner la confiance d'un tiers ou encore répandre un malware).
- gagner davantage (meilleur taux de réponse et / ou gains « unitaires » plus élevés).
- profiter d'une autre catégorie de victimes qui ne sont pas intéressées par les achats de biens ou services.
- profiter de l'effet de nouveauté : les victimes potentielles ayant appris avec le temps à reconnaître les messages publicitaires se laisseront plus facilement duper si le spam se présente sous une nouvelle forme moins reconnaissable et plus convaincante.
- déjouer (au début du moins) certains types de filtres anti-spam sachant reconnaître le langage caractéristique habituellement utilisé.

Ci-dessous, un panorama des principaux autres types de contenus véhiculés (l'objectif n'étant pas de détailler tout ce qui peut être transmis mais plutôt d'analyser les grandes tendances du spam tel qu'il se pratique actuellement). L'évolution de chaque type de contenu sera détaillée par la suite.



1.2.3.1 Gains en bourse

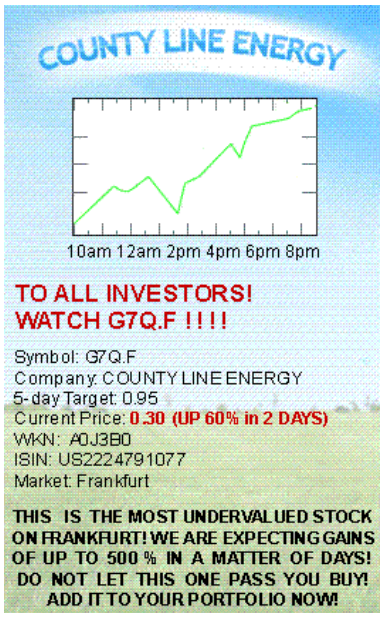
Autre source de revenus : la bourse. Largement utilisée, la technique « Pump and dump » également appelé « Stock dump » est une fraude financière. Elle est constituée de 3 phases clés :

1) Le fraudeur achète un certain volume d'actions. Il s'agit en général de titres cotés en centimes (appelés « penny stocks »), cela permettant d'atteindre des performances très élevées.
2) Une vaste campagne publicitaire est envoyée massivement à partir des canaux habituellement utilisés par le spam. Elle incite les destinataires à investir dans ce titre, le prétexte utilisé pouvant varier (rumeur de fusion avec un poids lourd du secteur, dépôt de brevet révolutionnaire, prévisions et conseils d'experts, etc.).
3) Sous l'effet des investisseurs crédules, le cours de l'action augmente brutalement (« pump »). Le fraudeur revend alors rapidement les actions détenues (« dump ») et empoche une forte plus-value, au détriment des malheureux investisseurs qui subissent la baisse du titre.

Cette méthode est très appréciée des spammeurs pour différentes raisons :

- Les gains sont importants (la performance du titre pouvant aisément atteindre 500%)
- Si la valeur du titre n'est pas influencée suite à un éventuel échec de la campagne publicitaire, la perte est minime : l'argent est habituellement investi dans des entreprises dormantes, le cours de l'action est donc stable (mais également plus influençable).
- L'encaissement de la plus-value se fait aisément, à l'inverse d'autres escroqueries pour lesquelles la collecte des revenus est plus problématique (comme pour le phishing).
- La technique est parfois réputée pour être plutôt anonyme, puisqu'il n'y a pas de véritable relation entre le spammeur et le spammé : les gains sont perçus indirectement et de façon « propre » puisqu'à partir du système boursier. Ce point est tout de même à relativiser, car les traces laissées par les ordres en bourse sont suspectes.

Une autre technique, nommée « Short and distort » désigne le processus inverse, à savoir profiter d'une baisse déclenchée artificiellement par la publication de rumeurs négatives.



Exemple d'un spam de type « pump and dump »

Une des premières fraudes financières de grande envergure de type « pump and dump » a eu lieu en 2004. Cette dernière a permis à deux citoyens canadiens d'empocher près de 23.4 millions de dollars après avoir fait monter le cours d'actions de deux sociétés (Absolute Health et Concorde America Inc). Jugés en 2005, les deux hommes ont été condamnés respectivement à des amendes de seulement 1.5 million de dollars et 650'000 dollars, ainsi qu'à deux interdictions relatives à d'éventuels types d'implications futures en bourse [MRGZ].

Selon Sophos, ce type d'annonce représentait en janvier 2005 moins d'1% des spams, tandis qu'elle s'élevait courant 2006 à 15% [SOPH01]. D'après BitDefender, ce taux atteignait 25% en 2007, un record qui classa cette fraude à la première place du classement annuel des 10 plus grandes menaces (suivi par les publicités pour médicaments, les messages à caractère pornographique et les montres contrefaites) [BITD].

Au vu des nombreux avantages offerts aux fraudeurs par cette méthode et à la crédulité habituelle des investisseurs en herbe, on peut manifestement conclure que seules des actions en justice systématiques assorties de peines exemplaires seront à même d'enrayer ce fléau.

1.2.3.2 Vol d'informations ou d'identités

Le moyen privilégié par les spammeurs permettant de soutirer des informations à des victimes est le « phishing ». Pour y parvenir, le pirate se fait passer pour une entreprise ou un site web (couramment une banque ou un service de transfert de fonds). Grâce à cette fausse identité, il incite la victime à révéler des informations personnelles sous un prétexte quelconque. Couramment, le message demande à la victime de saisir ses identifiants afin de réactiver son compte. S'il ne le fait pas, on lui fait croire que son compte sera clôturé.

La mise en œuvre la plus courante se base sur 2 éléments :

1) Un message dont l'identité de l'expéditeur est falsifiée, se présentant sous une apparence proche voir identique de ceux émis habituellement par l'expéditeur légitime et incitant le destinataire à se rendre sur un site web (un lien est inclus).
2) Le site web arborant le même design que celui de l'entité usurpée sur lequel la victime est priée de saisir son login et mot de passe. Les informations saisies sont ensuite transmises au pirate.

Une version primitive du phishing existe depuis fort longtemps : utilisée à l'époque par des « script kiddies » pour leur usage personnel, il n'était pas rare de voir ce genre de courriers sur certains services gratuits de messagerie, le formulaire permettant la collecte d'informations étant directement intégré au corps du message. Ce qui a évolué avec le temps, c'est d'une part son utilisation massive et à des fins lucratives, d'autre part le perfectionnement des techniques augmentant le taux de réussite (l'illusion étant plus convaincante).

Actuellement, des variantes moins courantes mais plus subtiles existent, basées sur des programmes malveillants spécifiquement conçus pour cette utilisation. Une fois exécuté par la victime, le programme s'installe dans son ordinateur. Il peut ensuite

reconnaître par exemple lorsque l'utilisateur se connecte sur le service d'e-banking de sa banque, pour le rediriger sur une copie conforme (en apparence du moins) et permettre par conséquent la collecte des informations saisies, directement exploitables par le pirate. Plus simple, il peut modifier la résolution DNS localement (par le fichier « hosts ») pour diriger les sites originaux sur des répliques pirates. A ce titre, une récente technique de DNS poisoning basée sur des serveurs DNS récursifs permet aussi de diriger les victimes sur de faux sites [SILI01] (cette variante du phishing étant parfois appelée pompeusement « phishing 2.0 »).

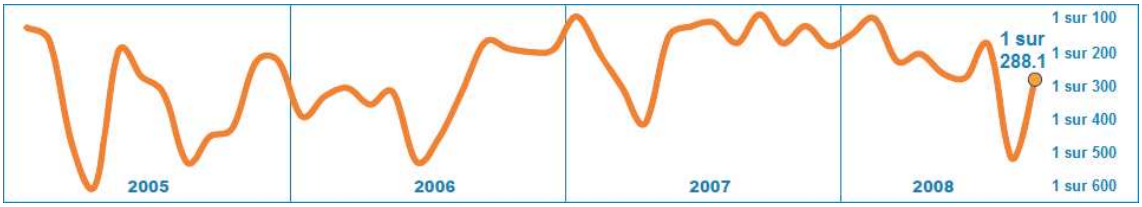
Un autre type de phishing voit le jour : le « spear-phishing ». Cette forme spécifique consiste à augmenter la crédibilité du message falsifié en y intégrant des informations personnalisées, telles que nom, prénom ou adresse du destinataire (récoltées par exemple à partir de réseaux sociaux). Appréciée pour réaliser des attaques ciblées, cette variante est peu courante dans le monde du spam, car elle requiert davantage de temps et de travail manuel, ce qui est relativement incompatible avec les méthodes expéditives des spammeurs qui privilégient la quantité à la qualité et au ciblage. Relevons tout de même que certains programmes malveillants sophistiqués ont fait leur apparition en 2006, lesquels permettent d'analyser automatiquement les courriers stockés sur l'ordinateur cible (dans le client de messagerie installé), afin d'en extraire un profil (organismes bancaires en contact avec la victime, noms, signatures, etc.). Le message falsifié est par la suite automatiquement personnalisé, ce qui permet d'atteindre un meilleur taux de réponse [TOMS]. 2 ans plus tard, l'utilisation de ce moyen reste marginale.

D'autres attaques virales permettant aussi le vol d'informations n'utilisent pas le phishing, notamment tous les programmes stockant les frappes au clavier (keyloggers).

A l'instar des manipulations boursières, le vol d'informations est très lucratif. Cependant, percevoir l'argent volé (à partir de comptes bancaires dont les informations de connexion ont été récupérées) est problématique. Pour cela, des personnes (appelées « mules ») font l'intermédiaire entre la victime et l'escroc en échange d'une commission (habituellement 5 ou 10%), l'objectif étant de rendre la traçabilité des fonds plus difficile.

Comme le montre une étude de MessageLabs, le taux de phishing durant des 4 dernières années est fortement instable, pouvant parfois varier d'un facteur 5 en l'espace d'un an. Malgré une année 2007 relativement affectée, ces fluctations, tant à la hausse qu'à la baisse ne reflètent globalement pas de tendance particulière en

terme de volume. Quoi qu'il en soit, même aux périodes ou le phishing était au plus haut, il représentait seulement 1% des messages transmis. En septembre 2008, il n'était selon MessageLabs que de 0.35%.



Si le phishing est tant redouté malgré de faibles volumes, c'est parce qu'il s'agit d'une attaque extrêmement dangereuse et fortement criminelle. Seuls quelques instants d'inattention ou une mauvaise connaissance des menaces sur internet peut conduire un internaute à de lourdes pertes financières. Il est important de préciser qu'en dépit d'une évolution peu inquiétante du volume transmis, les conséquences du phishing vont en empirant. A ce titre, une étude réalisée par l'institut Gartner illustre bien la situation actuelle [GART] :

- La perte moyenne par victime est plus faible en 2007 (886$) qu'en 2006 (1'244$).
- 3.3% des internautes américains recevant une escroquerie par phishing en 2007 se sont laissés leurrer, contre seulement 2.3% en 2006.
- La perte totale due au phishing aux Etats-Unis en 2007 s'élève à 3.2 milliards de dollars, contre 2.8 milliards en 2006.

L'augmentation du taux de réussite montre que :

- les messages sont toujours plus crédibles
- les internautes ne savent pas suffisamment reconnaître ces messages falsifiés.
- les protections anti-phishing couramment intégrées aux browsers actuels ne sont pas suffisantes (la durée de vie d'un site de phishing est toujours plus courte, la mise à jour de ces filtres n'est alors pas suffisamment rapide).

1.2.3.3 Promesses de rétributions

De nombreuses escroqueries se basent sur des promesses de rétribution. Les deux genres les plus connus sont :

- le scam nigérian (ou fraude 419)
- les loteries

Le scam nigérian (le terme « fraude 419 » vient du numéro d'un article du code pénal nigérian) est une ancienne escroquerie datant de la seconde moitié du XXème siècle et inspirée de la « Lettre de Jérusalem », une ancienne fraude datant de la fin du

XVIIIème siècle. Appliquée dans un premier temps aux moyens de communications de l'époque (courrier postal et fax), ces messages ont rapidement tiré parti des possibilités offertes par internet.

En quelques mots, cette arnaque est basée sur la crédulité des victimes (comme le plus grand nombre des attaques liées au spam) : le message demande de l'aide pour effectuer un transfert d'argent, en échange d'une commission (les sommes promises étant élevées). Pour débloquer les fonds, la victime est priée de réaliser un versement. Une fois ce versement réalisé, les contacts avec la victime sont coupés. Dans quelques rares cas, la victime fait le déplacement (généralement au Nigéria, voir dans certains autres pays d'Afrique). Elle se fait alors dépouiller (certains homicides ont aussi été recensés).

Représentant 8% des spam en mai 2003 selon BrightMail [JDN01], l'arnaque nigérienne est toujours active. D'après les études mesurant le scam global (c'est-à-dire phishing, scam nigérian et autres astuces), ce taux serait actuellement inférieur à 10% des spams.

Sur le même principe, les fausses loteries font miroiter le gros lot, et réclament en échange le paiement de frais administratifs ou de démarches de vérification.

1.2.3.4 Chantages & menaces

Le chantage est apparu comme nouvelle alternative au spam classique au cours des 4 dernières années. Comme nous le verrons ci-après, il est important de souligner que la forte majorité des chantages pratiqués s'appuient sur les évolutions technologiques récentes en matière de spamming, à savoir la conception de programmes malveillants évolués ainsi que l'existence de vastes réseaux « d'ordinateurs zombies » (botnets). Cela nous amène à la constatation suivante : la différence entre un spammeur et un escroc classique est toujours plus faible (cela se vérifie d'ailleurs pour l'ensemble des orientations prises par le spam ces dernières années). En effet, cette convergence est indéniable :

- Le spammeur tend toujours plus vers des pratiques criminelles. Ses activités commerciales dans la vente ne sont pas irréprochables puisqu'il s'agit souvent de produits contrefaits, mais ses clients obtiennent quelque-chose en échange de l'argent dépensé. Ce n'est plus le cas des nouvelles activités dans lesquelles il ne s'agit plus de clients mais de victimes qui ne tirent aucun gain de leur implication. En d'autres termes, le spammeur est passé en l'espace d'une dizaine d'années peu à peu du stade de vendeur à celui de voleur.

- Un escroc qui use de ces pratiques habituelles verra dans les technologies utilisées par le spamming un moyen de décupler sa puissance de frappe.

Au niveau des entreprises, le chantage utilisé pour leur soutirer de l'argent est de deux natures :

- menacer de révéler des informations sensibles si la rançon n'est pas payée. Les sources de ces données peuvent différer, mais l'utilisation de malwares couplée à la faiblesse probable de la sécurité au niveau des employés constitue généralement une bonne « porte d'entrée ».
- menacer de réaliser des attaques par déni de service (DoS) si la rançon n'est pas payée. Cette attaque réalisée par saturation des équipements de la société permet de rendre certains services indisponibles. C'est donc les botnets formés initialement pour l'envoi massif de spams qui sont utilisés pour cette tâche.

Ransomwares

Une autre technique particulièrement astucieuse datant de 2006 (premiers essais vers 2004) cible principalement les particuliers : le « ransomware ». Il s'agit d'un logiciel malveillant qui, une fois exécuté, recherche certains types de fichiers (.doc, .xls, etc.) puis les crypte. Il demande ensuite une somme d'argent à la victime en échange de la clé de décryptage. Si la victime n'obtempère pas, les donnes sont perdues car illisibles en l'état. Les cryptages employés dans les premiers ransomwares étaient peu robustes, ce qui n'est malheureusement plus le cas des dernières versions sorties en 2008. Si cette technique qui arrive peu à peu à maturité s'avère profitable, nous la verrons probablement se développer à l'avenir. Reste à savoir si les spammeurs sauront trouver le juste équilibre entre le montant de la rançon réclamé et la valeur des informations mises en péril.

Sur le même modèle se base le virus chinois « Kiazha », identifié par la société McAfee au début de cette année. Conçu pour infecter des équipements mobiles équipés de l'OS Symbian Series 60, ce programme composé d'anciens malwares menace l'utilisateur de rendre son téléphone inutilisable s'il refuse de payer 50 yuan (environ CHF 8.-) [GNT03].

De façon globale, les ransomwares peuvent aussi être utilisés contre des sociétés, mais cela est moins courant : le stockage généralement centralisé des informations et les backups réguliers offrent une bonne protection contre cette catégorie de menaces (mais l'attaque de certains terminaux mobiles pourrait changer la donne).

Kidnappings

Cas isolé mais représentatif des prétextes parfois insolites voir déplaisants utilisés, un spam émis à partir d'août 2008 annonçait « We have hijacked your baby ». Une rançon de 50'000$ était réclamée et une archive en pièce jointe était censée contenir une photo du bébé. Il s'agissait en fait d'un cheval de troie.

Menaces de mort

Début 2007, un spam faisait savoir au destinataire qu'un tueur à gages était chargé de son assassinat. 20'000$ étaient alors réclamés pour payer le tueur et ainsi lui éviter une pareille fin.

Cet exemple ainsi que celui du kidnapping atteste de la volonté des spammeurs de gagner de l'argent quelle que soit la gravité de leurs actes et le tort qu'ils peuvent causer : seule l'efficacité des méthodes compte, les limites de l'acceptable semblant constamment repoussées. Auparavant simples commerciaux peu scrupuleux, les spammeurs sont aujourd'hui de véritables malfaiteurs.

Torrents

A la même période que le spam annonçant un kidnapping, les spammeurs ont envoyé des emails annonçant à la victime qu'elle avait été surprise en train de télécharger des contenus protégés via BitTorrent. Le malware véhiculé en pièce jointe était présenté comme étant un rapport prouvant ces accusations.

1.2.3.5 Contenu contextuel

Le spam de s'oriente toujours plus vers l'emploi de prétextes en rapport avec l'actualité (les domaines étant variés). Voici quelques exemples :

- le tsunami dans l'océan indien (2005)
- le décès du pape Jean Paul II (2005)
- les attentats de Londres (2005)
- les événements en Birmanie (2007)
- l'éclipse lunaire totale (2008)
- les tensions entre les Etats-Unis et l'Iran (2008)
- la tournée mondiale de Madonna (2008)

L'objectif est le même : inciter l'internaute à prendre connaissance du message puis l'amener à cliquer sur un lien ou à ouvrir une page web permettant l'installation d'un malware.

Variante de ces prétextes, les spammeurs ciblent aussi certaines périodes de l'année (jour fériés, fêtes, etc.). C'est le constat de la société Barracuda Networks qui a relevé en 2007 une forte augmentation du phishing pendant Thanksgiving, plus précisément pendant les « Black Friday » et « Cyber Monday » (coup d'envoi des achats de fin d'année). Cela se produit aussi en début d'année, avec des offres promotionnelles axées par exemple sur les habituelles bonnes résolutions tel que la perte de poids [BAN].

1.2.3.6 Attaques virales

D'autres messages ont pour objectif d'infecter l'ordinateur d'un maximum de destinataires. Il ne s'agit bien entendu pas d'une fin en soi, mais plutôt d'une démarche préalable permettant d'atteindre ensuite d'autres objectifs tels que ceux décrits précédemment (voler des informations, constituer un réseau permettant de réaliser des envois en masse de messages publicitaires ou de mener des attaques DoS, etc.). Ces attaques virales se font directement à partir d'un fichier joint au message ou via un site web hébergeant le programme. Comme nous le verrons plus loin, une nouvelle technique appelée « drive-by-download » permet d'infecter un ordinateur lorsque l'internaute surfe sur le web, le tout en demandant un minimum d'intervention de sa part.

Le rapprochement ces dernières années entre les spammeurs et les développeurs a été un facteur déterminant dans les orientations prises par le spam. Il a contribué largement à renouveler et améliorer les méthodes utilisées, ce qui a conduit à une forme de spam toujours plus organisée et résistante. En effet, la volonté actuelle de concevoir de nouveaux moyens durables et efficaces contraste bien avec les techniques de l'époque construites sur l'exploitation des vulnérabilités « passagères ». A ce titre, on peut considérer que les attaques virales sont durables, puisqu'elles tirent généralement profit du facteur humain : à l'inverse des vulnérabilités techniques dont la durée de vie est restreinte (par l'application de correctifs), les faiblesses du facteur humain sont persistantes. Bien entendu, ces faiblesses jouent un rôle dans la première phase des attaques virales pendant laquelle on essaie d'exécuter le programme malveillant au moyen d'une erreur de l'utilisateur. Une fois installé, le programme remplit son rôle et se fait discret dans la majorité des cas.

1.2.4 Moyens employés par les spammeurs

Jamais à cours de nouvelles idées, les spammeurs renouvellent et améliorent perpétuellement leurs techniques. Cette section présente ces évolutions sous diverses perspectives.

1.2.4.1 Ciblage

En raison du coût dérisoire des messages envoyés, le spam est relativement peu ciblé. Cela représente en quelque sorte la démarche inverse de celle privilégiée par les publicitaires qui consiste à définir au mieux le public visé, afin d'atteindre un bon retour sur investissement dans la mesure où on économise en frais de publication / diffusion (ceci est aussi bien valable pour la publicité à la télévision que dans les journaux, ou également sur le web à condition que la facturation soit effectuée sur la base du nombre d'affichages).

Une autre raison explique le si faible ciblage du spam : le manque d'informations sur les destinataires, puisque les adresses spammées sont soit recueillies automatiquement sur le web (au moyen d'applications), soit générées par dictionnaire (assemblages de noms, prénoms ou initiales pour tenter de trouver des adresses valides).

Néanmoins, la tendance actuelle est d'améliorer d'une certaine manière ce ciblage en écrivant les messages dans la langue du destinataire. Comme décrit précédemment, le nombre d'internautes résidant en Chine a fortement augmenté à partir des années 2000. S'agissant d'une exceptionnelle réserve de consommateurs potentiels, les spammeurs ont alors commencé à cette époque à diffuser des messages rédigés en langue chinoise (il s'agissait de publicités pour la vente de logiciels pirates, de sites web chinois ou encore pour des équipements électroniques). Steve Linford, directeur général d'Ultradesign (un ISP installé à Londres), constate que le volume de ces messages apparus en décembre 1999 a violemment augmenté en janvier 2000. A cette période, il est même passé dans certains cas devant les spams en langue anglaise, comme le fait remarquer Dave Jacobs, ingénieur logiciel californien disant avoir reçu dans sa messagerie personnelle en moyenne 4 à 6 spams chinois par jour contre 1 ou 2 en langue anglaise [CNN].

De façon surprenante, une étude de la Cnil (portant sur 320'000 messages collectés en 3 mois) indique que seulement 8% des messages étaient rédigés en langues asiatiques en 2002, contre 84% pour ceux en langue anglaise et 7% en langue française (les autres langues étant très peu représentées) [CNIL02]. Cette propension

à employer l'anglais s'est poursuivie jusqu'en 2007 environ, McAfee annonçant que 99% des messages étaient alors rédigés dans cette langue. A l'inverse, l'éditeur annonce en 2008 que les langues utilisées sont toujours plus variées : seulement 23% des 104'000 messages collectés étaient rédigés en anglais, tandis que 15.2% étaient en portugais brésilien (il explique ce taux par l'adoption rapide des services d'e-banking au Brésil, rendant courantes les attaques par phishing bancaire envers les brésiliens) [JDN02].

Ecrire dans la langue du destinataire permet sans doute d'améliorer le taux de réponse, mais un problème de taille se pose aux spammeurs : les traducteurs automatiques régulièrement utilisés pour produire ces messages composent des textes de piètre qualité. Au vu de certains résultats aussi inintelligibles que peu crédibles, on peut réellement douter de l'efficacité de la méthode. Voici un extrait de spam promouvant la vente de logiciels en diverses langues [LNX02] :

> *« Com l'euro de logiciel est consacré possible une page Web, ils tous les usagers d'Internet avec le top logiciel de qualité pour les plus bas prix.*
>
> *Actuellement, nous offrons plus de 300 logicieux les plus populaires pour Windows et Macintoch télécharger le localisé pour l'anglais, l'allemand, le français, l'italien, l'espagnol et beaucoup d'autres langues, achat le logiciel OEM bon marché et économie einfach: »*

Evaluer les résultats apportés par ce type de messages est complexe. Quoi qu'il en soit, on s'aura certainement d'ici quelques mois si cette technique a porté ses fruits : si une méthode n'est pas ou plus assez satisfaisante, elle est rapidement abandonnée au profit d'une autre.

1.2.4.2 Vecteurs d'attaques

Destinés à être vus par le plus grand nombre, les spam voient leurs frontières régulièrement repoussées. Limité à ses débuts aux services de messagerie (dans un premier temps usenet, puis par email), le spam exploite à présent de nombreux autres canaux.

Blogs

Fréquemment utilisés, les blogs constituent l'un des « nouveaux » vecteurs d'attaques employés par les spammeurs.

Le spamming via les blogs est réalisé de 3 façons :

- à partir de blogs ouverts et détenus par les spammeurs (appelés « splogs).

- dans les commentaires des messages
- via les trackbacks (ou « rétroliens »)

L'objectif premier d'un splog est de publier des liens vers d'autres sites malveillants, ce qui influence artificiellement leur popularité et par voie de conséquence leur positionnement dans les moteurs de recherche (principe des « backlinks », utilisés entre autres par Google pour déterminer en partie le PageRank d'une page web, indice déterminant dans le classement des résultats).

Ces services de publication de blogs sont très prisés des spammeurs car :

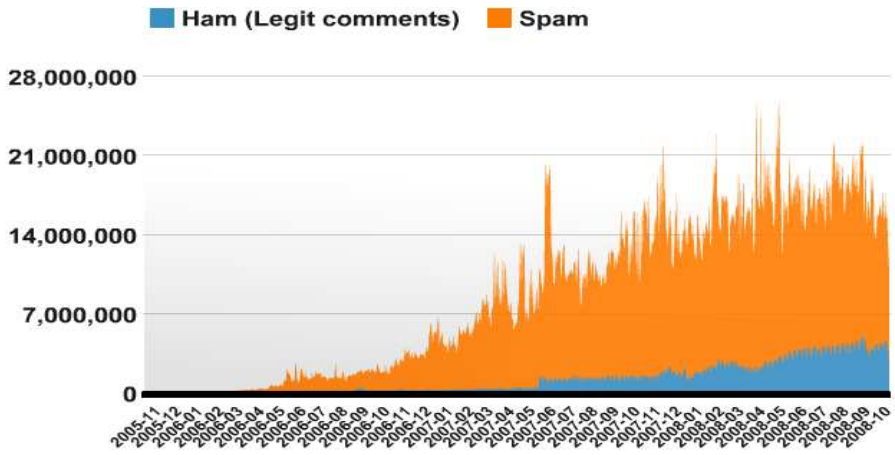
- ils sont gratuits (les autres services payants sont très peu utilisés)
- les spammeurs ont trouvé des moyens de créer automatiquement de grandes quantités de comptes (lorsqu'un d'entre eux est fermé, il y en a d'autres pour assurer la relève)
- leur réputation n'est plus à faire, ce qui permet à priori de dissimuler plus facilement des contenus frauduleux dans un service habituellement considéré comme « propre ». De ce fait, ils sont rapidement indexés aux moteurs de recherche, occupent plus aisément de meilleurs classements et tirent profit des services annexes offerts (en particulier les annuaires).
- il est difficile pour les administrateurs de ces services de différencier les vrais blogs des splogs.

Pour crédibiliser ces faux blogs et attirer des visiteurs susceptibles de cliquer sur les liens, les spammeurs les alimentent en contenu provenant d'autres sites ou blogs (via des flux RSS).

Les deux autres techniques sont différentes de cette première, dans la mesure où les spammeurs polluent un espace qui ne leur appartient pas : ils touchent donc potentiellement tous les visiteurs occasionnels ou réguliers du site en question. Poster des liens sur ces espaces leur permet, comme pour la méthode des splogs, d'améliorer aussi leur positionnement dans les moteurs de recherche par la création artificielle de liens.

Les premières tentatives de création de splogs datent de 2003. En octobre 2005, elles ont littéralement explosé sur certains services de publication, conduisant Google Blogger à supprimer 13'000 splogs à cette période. Selon une étude de l'université du Maryland datant de mai 2006, 56% des blogs anglophones seraient des splogs [EXP].

En léger recul ces derniers mois, la situation du spamming via les commentaires des blogs est tout de même de façon générale en forte progression, comme le témoigne la statistique suivante publiée par Akismet (service anti-spam spécialisé dans le filtrage des commentaires sur les blogs) [AKI] :



Forums, wikis et livres d'or

De par la facilité avec laquelle il est possible d'ajouter ou de modifier des contenus sur ces types de plateformes collaboratives, ces services sont aussi touchés par le spam.

La vulnérabilité de ces espaces peut largement varier en fonction des configurations. Certains forums laissent par exemple les visiteurs non identifiés créer des topics ou poster des réponses (de plus en plus rare), d'autres rendent la création d'un compte obligatoire pour ces actions. En fonction des protections mises en œuvre, ce processus d'inscription est plus ou moins rédhibitoire pour les spammeurs (qui procèdent à des inscriptions automatiques). Il en est de même pour les wikis (les livres d'or sont potentiellement toujours des cibles, mais ils sont rares car relativement désuets).

Malgré le manque d'études à ce sujet, on peut s'apercevoir en pratique que ce vecteur d'attaque est toujours d'actualité. De surcroit, les protections empêchant les inscriptions automatiques sont plus vulnérables qu'auparavant, ce qui expose d'avantage ces services.

Téléphonie mobile

Les premiers cas de spams par SMS constatés en France ont eu lieu en 2002. Une vaste diffusion de messages incitait les destinataires à appeler un numéro surtaxé. D'après les estimations de la CNIL, 3 millions de SMS ont été envoyés rien que pour le département des Hauts-de-Seine, ce qui a conduit à 180'000 appels vers le numéro surtaxé en question [JDN03].

Alors que le spam via SMS envahissait le Japon en 2004 (l'opérateur NTT DoCoMo ayant du prendre des mesures), il a fallu attendre cette année pour le voir réapparaitre en France. Abondamment envoyés en début d'année et jusqu'à présent, le principe est identique : inciter les destinataires à appeler un numéro surtaxé. De nombreuses

personnes ont perdu plus ou moins d'argent, soit en appelant ce numéro, soit en essayant de se désinscrire (par le mot clé « STOP »).

Autre technique de spamming via téléphones mobiles, cette fois-ci aussi originale qu'anecdotique, l'envoi de publicités via Bluetooth. Selon la « Mobile Marketing Association » (MMA), laisser la liaison Bluetooth de son téléphone active et en mode visible devrait signifier qu'on est d'accord de recevoir de la publicité par ce biais. Pour l'instant, la diffusion de contenus publicitaires via Bluetooth n'est pas encore à l'ordre du jour. En raison des limitations de cette technologie (en particulier à cause de la faible portée des émissions), le Bluetooth sera tout au plus utilisé par quelques publicitaires dans certains lieux publics, mais son utilisation en tant que nouveau canal de diffusion du spam est très peu probable.

Autres services en ligne

A l'instar des services de publication de blogs, d'autres services en ligne sont parfois utilisés de façon détournée. C'est entre autres le cas de Google Docs ayant servi à héberger des contenus publicitaires. Autre service touché : Google Calendar. Des escrocs ont émis des messages (en particulier des scams nigérians) sous forme de rendez-vous (cela permettant d'échapper aux filtres anti-spam).

Ces types de diffusion ont eu lieu en 2008 et confirment bien la tendance actuelle (amorcée fin 2007) visant à limiter les pièces jointes au profit des contenus hébergés en ligne et accessibles généralement via un lien. Cette nouvelle approche offre plusieurs avantages :

- les internautes seraient plus enclins à cliquer sur un lien plutôt que d'ouvrir un fichier joint (la sensibilisation aux risques fait lentement son chemin et conduit les utilisateurs à prendre conscience du risque viral couru par l'ouverture d'un fichier)
- ces fichiers joints requièrent des logiciels adaptés que l'utilisateur doit avoir installés préalablement sur son poste (Microsoft Office, Adobe Reader, etc.)
- stocker des contenus sur des sites réputés dignes de confiance offre une meilleure chance de passer à travers les filtres anti-spam.

Autres plateformes matérielles

Jusqu'à présent restreints aux PC, les spammeurs ont commencé à s'intéresser en 2007 aux utilisateurs d'ordinateurs Apple, en adaptant les outils de phishing. Ce n'était pas la première fois que des malwares étaient conçus pour des équipements de ce type, mais la volonté des spammeurs d'exploiter ces postes était nouvelle (ils

préféraient auparavant se contenter du nombre gigantesque de PCs exploitables sans avoir à adapter les programmes).

Selon les estimations de Sophos, d'autres plateformes seraient susceptibles d'attirer l'attention des pirates, en particulier les terminaux mobiles équipés en liaisons WiFi (PDA, netbooks, etc.) [SOPH01]. Des chercheurs du Georgia Tech vont jusqu'à prédire l'apparition possible à l'avenir de botnets formés d'équipements mobiles communicants en raison de leur démocratisation croissante, leur manque de protection contre les programmes malveillants, la faible diversité des OS embarqués et les failles de sécurité qu'ils peuvent engendrer [GNT01]. Cette hypothèse ne semble toutefois pas réellement plausible dans un futur proche.

1.2.4.3 Formats

Dans l'intention de passer à travers les filtres anti-spam, les spammeurs ont modifié à de nombreuses reprises leurs façons de véhiculer du contenu par email.

Jusqu'en 2005, la quasi-totalité des spams envoyés par email étaient au format texte. A cette période, un nouveau format est apparu : le spam image. Occupant selon McAfee 10% du total des spams fin 2005, il a pris de l'ampleur et s'élevait à 40% en novembre 2006.

Cette même année, les spammeurs ont apporté de nombreuses améliorations à ce format afin de le préserver au mieux des solutions anti-spam. La société Commtouch publie dans un rapport de 2006 la nature de ces innovations [COM] :

- pixels de couleur et de position aléatoires ajoutés dans le fond de l'image
- changements de couleur des bords, du fond ou de la police d'écriture
- découpage de l'image de base en plusieurs images, affichées de façon recomposée
- images GIF animées
- utilisation d'autres formats que les classiques GIF et JPG (PNG par exemple)
- ajout de texte aléatoire récupéré à partir de sites légitimes
- répartition aléatoire de motifs sur l'image
- textes déformés, retours à la ligne aléatoires, lettres collées
- coloration du fond avec diverses couleurs
- caractères multicolores et de hauteurs aléatoires

En 2007, le spam image connaît son apogée avec 60% du total des spams, contre seulement 20% de spams texte (selon BitDefender [BITD]).

La même année, de nombreux autres formats ont été utilisés, mais aucun d'entre eux n'a réellement duré. Parmi ces tentatives, citons le spam au format PDF : débuté en juillet 2007, il atteignait selon Sophos 8% à la mi-août 2007 [SOPH01], avant de disparaître fin août. Egalement en juillet 2007, des spams au format Excel ont été envoyés, remplacés 3 mois plus tard par le spam MP3. Ce dernier a atteint 7 à 10% du total des spams avant d'être délaissé comme ses prédécesseurs. Enfin, l'année 2007 s'est terminée avec une dernière tentative infructueuse basée sur des spams vidéos (accessibles via un lien dans l'email).

En raison de l'amélioration des solutions contre le spam image, ce dernier efficace jusqu'à présent a rapidement perdu de intérêt, conduisant les spammeurs à abandonner précipitamment ce format en 2008 au profit du texte, apprécié pour sa taille réduite et sa grande adaptabilité (automatique, par substitution synonymique, reformulation, formatage des mots, etc.). Selon BitDefender, le spam image représentait mi-2008 seulement 3% contre 70% pour le spam texte. Les autres formats ne comptent plus que pour 10 à 15% du total des spams.

Ajoutons pour terminer que l'éditeur Symantec annonce une récente tentative de retour au spam image. Il est ainsi passé de 1.6% en août 2008 à 2.6% en septembre, atteignant 8.6% pendant les 10 premiers jours d'octobre 2008. Toujours selon Symantec, de récentes attaques par phishing utilisant le spam image n'ont pas prouvé leur efficacité face aux solutions anti-spam [SYM02]. On peut donc manifestement s'attendre à un nouvel abandon du format.

1.2.4.4 Botnets

Cité à de nombreuses reprises dans ce travail, un botnet est un réseau constitué de machines contaminées par un programme malveillant (de type backdoor) permettant au pirate de les contrôler à distance. Ce pilotage en masse permet d'ordonner à l'ensemble des membres du réseau la réalisation d'une certaine tâche. Les utilisations les plus courantes sont l'envoi de spams ou les attaques par déni de service distribué (DDoS) qui permettent de submerger une cible dans le but de la rendre inopérante. Les ordinateurs dont la contamination a pu être réalisée de différentes façons (pièces jointes par email, téléchargement sur le web ou en peer-to-peer, etc.) appartiennent en général à des particuliers qui ignorent la présence de ce programme malveillant ainsi que l'utilisation frauduleuse de leur équipement par les cybercriminels.

Non seulement le pirate bénéficie de la puissance offerte par l'asservissement d'une grande quantité de machines, mais aussi d'une certaine anonymisation : chaque

ordinateur laisse ses propres traces (dans des logs lors d'attaques DoS, dans les en-têtes d'emails, etc.), il est de ce fait difficile de savoir qui est réellement à l'origine de l'attaque.

Technique datant d'une dizaine d'années, les botnets sont montés en puissance au cours des dernières années, rassemblant toujours plus d'ordinateurs. Néanmoins, les experts constatent récemment que les spammeurs préfèrent actuellement créer un grand nombre de petits réseaux, comme l'explique Mika Stalhberg de la société F-Secure :

> *« La plupart des botnets sont contrôlés par IRC (Internet Relay Chat). Le problème de leurs auteurs est que, si le serveur IRC central n'est plus en activité, ils perdent leur botnet en intégralité. Ces individus ne veulent donc pas mettre tous les oeufs dans le même panier, et font désormais tourner de plus petits botnets. »* *[GNT02]*

D'après Joe Steward (directeur section malwares chez SecureWorks), le plus grand botnet actuellement en service nommé « Srizbi » contrôlerait 315'000 machines capables d'envoyer 60 milliards de spams par jour. Vient ensuite « Bobax » avec 185'000 ordinateurs et 9 milliards de spams journaliers. De façon générale, les 11 plus gros botnets contrôleraient au total plus d'un million d'ordinateurs responsables de 100 milliards de spams par jour [PCWD].

Ayant succédé à la vieillissante technique basée sur les relais ouverts, les botnets ont permis aux spammeurs d'atteindre des volumes de spams colossaux tout en disposant d'un outil fiable et exploitable durablement : à l'inverse des relais ouverts où le spammeur est tributaire de leur « durée d'exploitation » ou des difficultés à en trouver davantage, constituer un réseau d'ordinateurs est une meilleure solution pour différentes raisons :

- un ordinateur contaminé va certainement le rester pendant longtemps. En effet, les programmes malveillants se font discrets, particulièrement les récents qui vont jusqu'à limiter la charge CPU.
- si certains utilisateurs se débarrassent du programme intrus, la performance du réseau est infiniment peu affectée en raison du grand nombre d'équipements
- le réseau est constamment alimenté en nouveaux ordinateurs, d'où un gain en performance
- on profite de l'effet « boule de neige » : toujours plus d'ordinateurs contrôlés permettent d'envoyer toujours plus de spams, certains étant destinés à contaminer d'autres machines en vue d'enrichir le réseau. Des mécanismes spécifiques améliorent aussi la propagation du malware (exploitation du carnet d'adresses de la victime par exemple)

- les moyens de combattre ces réseaux ne sont pour l'instant pas suffisamment satisfaisants.

1.2.4.5 Supercheries

Les internautes sont aujourd'hui de plus en plus conscients des risques et pièges d'internet. Pour contrer cette vigilance, les spammeurs font preuve d'une grande inventivité et mettent au point différentes astuces afin de tromper un maximum d'internautes. Voici quelques exemples de supercheries utilisées ces dernières années imageant bien l'exploitation récurrente des brèches sécuritaires causées au niveau humain (ingénierie sociale).

Rapports de non-remise (NDR)

Cette supercherie utilise un type de message bien connu des internautes : le rapport de non-remise (reçu automatiquement lorsqu'un message envoyé n'a pas pu être remis correctement. Profitant de la réputation « inoffensive » des ces messages, les spammeurs incitent une partie des destinataires à ouvrir de tels messages qui ne présentent à priori pas de risque.

Cette astuce ancienne à été utilisée à nouveau en 2008. Symantec a constaté en mai une vague de faux emails de non-remise [SYM01]. Pour générer des NDR plus vrais que nature, la technique employée est habile : au lieu d'être placée dans le champ « À », l'adresse du destinataire est insérée dans le champ « De » (tandis que le champ « A » comporte une adresse aléatoire inexistante). L'effet est le suivant : une fois que le message a été acheminé jusqu'à sa prétendue destination, un message NDR est généré (puisque l'adresse n'est pas valide) puis envoyé à l'adresse mentionnée de l'expéditeur. Puisque cette dernière a été falsifiée par le spammeur, le « vrai destinataire » reçoit un spam lui faisant croire qu'un de ses emails émis n'a pas atteint sa destination. Suivant la configuration du serveur ayant généré le NDR, le véritable contenu du spam est inclus au message (l'objectif de faire lire le spam est donc atteint, à condition que le destinataire se soit laissé piéger par l'apparence trompeuse de l'email).

Une version inspirée des NDR a été repérée par BitDefender plus tard dans l'année, vers août 2008 [PSZO]. Un message se faisant passer pour FedEx informait le destinataire que son colis envoyé un mois plus tôt n'avait pas pu être livré. Pour permettre la récupération du colis, l'utilisateur est invité à ouvrir et imprimer un document fourni en pièce jointe (format .zip). Si l'internaute s'exécute, il infectera son ordinateur d'un programme malveillant capable de récupérer des frappes au clavier, générer des captures d'écrans, désactiver un éventuel pare-feu, etc.

Faux utilitaires (rogues)

Faire croire à l'utilisateur qu'on lui veut du bien est une technique efficace, particulièrement auprès des utilisateurs lambda. Le principe est simple : un programme malveillant se présente sous l'apparence d'une solution anti-spyware ou anti-virus (en version d'essai). Il déclenche alors de fausses alertes et incite l'utilisateur à payer pour acquérir la version complète de la solution logicielle. Non seulement les informations bancaires de la victime sont dérobées lors du paiement, mais son ordinateur est généralement intégré à un botnet.

Selon G-DATA, cette menace inonde actuellement le web et pourrait s'amplifier les prochains mois [GSMO1].

Fausses sécurités

Dès l'instant où des services « sensibles » tel que l'e-banking se sont démocratisés sur internet, les utilisateurs ont été sensibilisés à l'importance du célèbre logo de cadenas affiché par le browser. Vérifier que ce logo est affiché (de même que la présence du « https:// ») lorsqu'on accède à ce type de services a été présenté durant longtemps (et c'est parfois toujours le cas actuellement) comme offrant une garantie sécuritaire.

Malheureusement, il n'en est rien. Il est en effet possible de mettre en place une liaison sécurisée via SSL sans recourir à une autorité de certification agréée. Le certificat ainsi généré est donc auto-signé, ce qui permet aussi l'affichage du cadenas et de la mention « https:// ».

Les spammeurs ont alors créé vers 2005 de tels certificats qu'ils ont appliqués à leurs sites de phishing. La victime pensant être connectée à son service d'e-banking habituel vérifie la présence du cadenas et saisit ensuite son login en toute quiétude.

1.2.4.6 Vérification des adresses email

Les moyens utilisés pour vérifier la validité d'une adresse email se sont multipliés au cours du temps. Actuellement, pas de réelle innovation mais une tendance au mixage de plusieurs techniques dans un seul mail, comme l'annonce l'éditeur Bitdefender dans un communiqué de presse datant d'octobre 2008 [BITD]. Pour information, les 3 méthodes utilisées conjointement pour vérifier la validité d'une adresse sont :

- la demande d'un accusé de réception
- l'utilisation d'un lien vers une image permettant la validation de l'adresse
- l'insertion d'un faux lien de désinscription

1.2.4.7 Redirection d'adresses

Les liens insérés dans les spams sont très largement utilisés quel que soit l'objectif (vente de produits, phishing, infection par malware, etc.) mais ils causent régulièrement l'interception du message par les anti-spams.

Pour limiter les pertes causées par ces filtres, l'éditeur Sophos a remarqué une nouvelle technique début 2007 [SOPH01] : l'utilisation d'un site légitime piraté en tant qu'intermédiaire entre le message du spammé et le site du spammeur.

La technique est composée de 3 étapes :

1) un site web est piraté
2) le spammeur stocke sur ce site une page permettant la redirection vers un autre site
3) un lien vers cette page est inséré à l'email. Lorsque l'utilisateur clique dessus, il est conduit sur le site légitime. Ce dernier va alors rediriger l'internaute sur le site du pirate préalablement défini dans la page de redirection. Pour la solution anti-spam analysant le contenu du mail, le site en question désigné par le lien se présente comme étant digne de confiance.

En dehors du problème lié au filtrage de ce type de liens, le site piraté subit un préjudice non-négligeable qui peut l'amener à être blacklisté.

1.2.4.8 Vulnérabilités des Captcha

Un Captcha (acronyme de « Completely Automated Public Turing test to tell Computers and Humans Apart ») est comme son nom l'indique un système appartenant à la famille des tests de Turing permettant de différencier un humain d'un ordinateur. Il est couramment utilisé sur le web pour interdire la création de comptes de façon automatique.

Les captcha utilisés par les plus grands services (Yahoo, Google, Windows Live, etc.) ont tous été cassés, pour la plupart au début 2008. L'efficacité des algorithmes de cassage varie selon les cas. Pour les captcha de Google, le taux de réussite serait d'environ 20% soit suffisamment pour créer des comptes en masse.

A partir de ces comptes, les spammeurs disposent par conséquent d'adresses fraîches et non blacklistées utilisables pour l'envoi de spams. Une fois repérées, elles sont abandonnées et aussitôt remplacées par d'autres.

Malgré leur efficacité relative, les captcha sont toujours couramment utilisés. Les plus grands services améliorent leur complexité et cherchent des solutions alternatives. On

trouve par exemple des captcha plus complexes (deux mots, variation de la couleur du texte par rapport au fond, lignes et pixels parasites), des calculs à résoudre, des messages audio, des mosaïques d'images qu'il faut sélectionner « par familles », etc.

1.2.4.9 Drive-By-Download

Cette technique apparue fin 2006 permet d'infecter une machine avec un minimum d'intervention de la part de l'utilisateur.

Pour parvenir à ce résultat, des pages web conçues dans ce but tentent d'exploiter des vulnérabilités de l'ordinateur cible. Si ce dernier en comporte, un programme appelé « trojan downloader » est installé automatiquement et de façon tout à fait silencieuse. Il se charge ensuite de télécharger puis d'installer d'autres malwares sur le poste.

Il est possible d'exécuter un tel script malveillant en ouvrant un lien inséré dans un spam ou simplement en surfant sur le web, même si le site en question est habituellement digne de confiance : certains sites à grand trafic sont piratés, d'autres exécutent du code malveillant à leur insu à travers leur système d'affichage publicitaire.

Cette technique actuellement en pleine expansion représente un risque très important puisqu'un internaute peut se retrouver piégé sans même ouvrir un fichier. Faire attention à ce que l'on ouvre n'est donc plus suffisant, il faut aussi maintenir un système propre et à jour (bonne pratique bien peu appliquée par les privés).

1.3 Evolution des solutions

1.3.1 Solutions techniques

En raison de l'ampleur prise par le spam, de nombreuses sociétés (certaines provenant du domaine des anti-virus) se sont rapidement intéressées à ce nouveau marché. Les solutions anti-spam ainsi créées sont donc devenues rapidement gênantes pour les spammeurs qui ont été contraints de s'adapter à ces nouveaux obstacles.

Cela pose un problème majeur : les éditeurs anti-spam travaillent de façon réactive. Les spammeurs ont alors toujours une longueur d'avance. Cela explique d'ailleurs pourquoi la nature des attaques est fortement cyclique : lorsque les spammeurs ont trouvé un moyen de contourner les solutions en place, ils l'exploitent au maximum et prennent de cours les éditeurs anti-spam. Une fois les outils anti-spam adaptés, le taux de réussite de la technique décline et les spammeurs passent à autre-chose. Certaines

techniques abandonnées refont parfois surface quelques temps plus tard, cela dépend de leur efficacité.

Les éditeurs de solutions contre le spam travaillent de façon réactive car :

- une approche proactive est difficilement envisageable (on ne peut manifestement pas prévoir efficacement les nouvelles orientations prises par les spammeurs).
- ils n'ont aucun avantage à anticiper les spammeurs car cela reviendrait à tuer la « poule aux œufs d'or ». A ce titre, leur situation est ambigüe : ils doivent proposer des solutions suffisamment efficaces pour donner satisfaction à leurs clients (et rester crédibles face à la concurrence), mais ne doivent pas pour autant éradiquer toute forme de spam, ce qui les conduirait inexorablement à leur perte. D'ailleurs, précisons qu'ils ne traitent pas l'origine du problème mais seulement ses conséquences. Puisque les internautes ne sont pas tous correctement protégés et que les solutions anti-spam sont perfectibles, le marché du spam reste profitable.

On constate donc que les solutions anti-spam évoluent exactement au gré des nouveautés initiées par les spammeurs. De façon générale, on peut résumer cette progression de la façon suivante :

- Les menaces se diversifient, ce qui oblige les solutions anti-spam à intégrer des techniques toujours plus nombreuses et variées.
- Les menaces sont plus subtiles et difficiles à contourner qu'à l'époque. Leur maîtrise nécessite alors des filtres plus intelligents.
- La course effrénée entre spammeurs et solutions anti-spam rend les outils toujours plus complexes.
- Les progrès de la lutte anti-spam sont neutralisés par ceux des spammeurs. Du côté de l'utilisateur, l'amélioration ressentie n'est pas toujours flagrante.
- La multiplication des moyens de protection n'est pas sans risque. Certaines solutions ont des effets pervers. C'est par exemple le cas des systèmes anti-spam basés sur l'authentification de l'expéditeur, qui peuvent causer des avalanches de mails « légitimes » à destination des ISP dont les services ont été détournés (le site LesNouvelles.net annonçait fin 2006 que ce type de messages représentait entre 15 et 30% du volume de spams rejetés par jour [LENO]). Dans une moindre mesure, les solutions actuelles génèrent toujours des faux positifs, préjudiciables dans certains cas. Autre exemple : les systèmes basés sur des listes noires ont quant à eux été vivement critiqués depuis longtemps pour leur gestion parfois discutable (pool d'adresses abusivement bannis, difficulté à faire retirer une entrée des listes, etc.).

1.3.2 Recours juridiques possibles et condamnations

L'absence de base légale solide de par le passé permettait généralement aux spammeurs d'agir en toute impunité. Toutefois, l'adaptation des lois ont permis de

clarifier ces comportements répréhensibles, ce qui constitue à présent une nouvelle menace envers les spammeurs.

Cette partie traite des principales lois en vigueur aux Etats-Unis, en France et en Suisse, ainsi que leurs différences respectives. Enfin, une partie détaille l'évolution des condamnations.

1.3.2.1 Evolution des lois

En fonction des pays, les nouvelles dispositions prises en vue de lutter contre le spam ont eu lieu à des époques différentes.

Mises à part certaines révisions de lois ayant eu lieu avant 2000 (telles qu'en Italie, en Autriche ou en Finlande), les adaptations de la législation aux problèmes causés par le spam sont véritablement apparues à partir de 2002. Voici quelques dates illustrant ces évolutions :

- L'Union Européenne s'est pourvue en juillet 2002 d'une loi sur la protection de la vie privée dans le secteur des communications électroniques [CNIL03].
- La France a adopté le 21 juin 2004 la loi pour la confiance dans l'économie numérique (LCEN) [CNIL04].
- Aux Etats-Unis, la loi « Can-Spam » a été adoptée par le Congrès en 2003 et est entrée en vigueur le premier janvier 2004.
- La Suisse a appliqué à partir du 1er avril 2007 une révision de la loi sur les télécommunications (LTC) [MCL].

Naturellement, d'autres lois antérieures au spam existent et s'appliquent toujours (c'est par exemple le cas de la loi du 6 janvier 1978 de la Cnil qui oblige les sociétés à déclarer leur fichier d'adresses). Néanmoins, ces révisions permettent de combler certains manques.

1.3.2.2 Opt-in & opt-out : 2 approches

La notion d'opt-in ou d'opt-out est fondamentale du point de vue juridique car elle contribue à définir ce qui est légal et ce qui ne l'est pas.

L'opt-in oblige les publicitaires à obtenir le consentement préalable des destinataires avant de leur envoyer de la publicité, tandis que l'opt-out autorise l'envoi de publicités sans leur consentement préalable (il s'agit donc d'un accord tacite, mais le destinataire est en droit de demander de ne plus recevoir de publicité).

L'opt-in est donc plus contraignant pour les publicitaires et privilégie la protection des internautes. Ce principe est appliqué aux pays de l'Union Européenne depuis 2002

(directive n° 2002/58/) et à la Suisse depuis 2007 (révision de la loi sur les télécommunications (LTC)).

La France et la Suisse appliquent tout de même l'opt-out dans certains cas.

En France, les conditions pour être soumis à l'opt-out sont les suivantes [DDM] :

- prospecter auprès de personnes morales (toutefois, l'opt-in s'applique si l'adresse email professionnelle permet d'identifier un individu)
- prospecter dans le cas d'une relation post contractuelle, à condition que :
    - les coordonnées du destinataire proviennent directement de lui, dans le cadre d'une vente ou d'une prestation de service
    - les produits ou services proposés soient similaires à ceux vendus antérieurement
    - le destinataire dispose d'un moyen lui permettant de s'opposer à l'exploitation de ses coordonnées (gratuitement, simplement, et à chaque prospection)

En Suisse, les conditions pour être soumis à l'opt-out sont similaires [SBZ] :

- prospecter auprès de clients existants, à condition que :
    - leur adresse provienne d'eux-mêmes et par le biais d'une commande
    - la publicité vise des prestations, marchandises ou services analogues.
    - le nom du destinataire soit correctement indiqué, et qu'il dispose d'un moyen lui permettant de s'opposer à la réception de tels courriers.

L'opt-out, beaucoup plus permissif envers les publicitaires est le modèle appliqué par les Etats-Unis dans leur loi fédérale CAN-Spam adoptée par le Congrès en 2003 et entrée en vigueur le 1er janvier 2004.

1.3.2.3 Conditions légales régissant l'envoi massif de publicités

Les exigences devant être appliquées pour envoyer légalement des campagnes publicitaires en masse sont très semblables entre les pays. Elles s'articulent généralement autour des règles suivantes :

- le principe opt-in / opt-out (en fonction du pays) doit être respecté
- l'identité de l'expéditeur doit être exacte (ni camouflée, ni falsifiée).
- chaque message publicitaire doit permettre au destinataire de refuser l'envoi futur de messages (cette possibilité devant être claire, facile et gratuite).
- les méthodes de collecte irrégulières d'adresses email sont proscrites

1.3.2.4 Condamnations & impact des lois sur le spam

De nombreuses condamnations de spammeurs ont lieu aux Etats-Unis. Débutées peu de temps après l'adoption de la loi CAN-Spam, elles sont courantes et particulièrement sévères. Non seulement les amendes sont pharaoniques (couramment plusieurs millions de dollars), mais les spammeurs sont souvent condamnés à des peines de prison pouvant atteindre parfois la dizaine d'années. Cette année, le spammeur multirécidiviste Eddie Davidson est même allé jusqu'à se suicider alors que plusieurs condamnations lui avaient été infligées [SILI02].

Malgré l'apparente « efficacité » du système juridique, deux problèmes se posent.

Le premier concerne le manque d'impact sur le marché du spam. En effet, 4 ans après l'introduction de la loi étatsunienne, tous les indicateurs sont au rouge. Les spams montent en puissance, deviennent toujours plus dangereux et les volumes transmis sont démesurés. Comme le disait John Levine (auteur d'« Internet pour les nuls ») début 2005, les spammeurs n'ont pas fait d'efforts pour se conformer aux règles de la loi CAN-Spam [WASH]. Cela leur aurait pourtant permis de poursuivre leur activité lucrative sans risquer de s'attirer les foudres de la justice (mais au prix d'un gain financier certainement moindre).

Comme le faisait remarquer Michael Osterman (président d'« Osterman Research Inc. »), les spammeurs ont recours à des dizaines d'astuces leur permettant de devenir anonymes sur le web [WASH]. Cela expliquerait alors pourquoi l'appât du gain l'emporterait sur la menace juridique. Avec le développement des botnets, cette hypothèse semble actuellement toujours parfaitement crédible.

Le deuxième problème est apparu récemment, en septembre 2008. La Cour Suprême de Virginie vient d'acquitter Jeremy Jaynes, l'un des premiers spammeurs condamnés (en 2004). Il était accusé d'avoir envoyé près de 10 millions de spams par jour, via les serveurs d'AOL [DLM].

Selon la Cour, la loi CAN-Spam serait anticonstitutionnelle :

> *« Cette loi dévoile en fait son visage anticonstitutionnel car elle interdit la transmission, anonyme et en masse, d'email non-sollicités, incluant ceux à caractère politique, commercial ou de quelconque nature, protégé par le Premier Amendement de la Constitution des Etats-Unis »*

Selon les juges, la distinction entre la diffusion de messages commerciaux et celle de messages d'une autre nature ne serait pas suffisamment claire.

Des attaques similaires accusant la loi d'être anticonstitutionnelle ont déjà eu lieu fin 2004. Selon la tournure prise par ces événements et la position adoptée par la Cour Suprême des Etats-Unis, le cadre juridique de la lutte anti-spam pourrait se détériorer.

En France, les condamnations sont rares et clémentes : une entreprise poursuivie par la Cnil en 2002 a été condamnée à 3'000€ d'amende par la Cour de cassation en 2006, un spammeur a été condamné en 2003 à 1'010€ d'amende, un autre en 2004 à 22'000€ d'amende.

1.4 Quel avenir pour le spam ?

Les prévisions concernant l'avenir du spam sont nombreuses, et il n'est par rare de remarquer à posteriori qu'une grande partie d'entre-elles n'étaient pas exactes.

Citons par exemple un article du journal « Le Temps » qui titrait en septembre 2002 « *Le spam est en train de couler Internet* » [LTPS]. Le « faible » 32% de spams (par rapport au « modeste » volume total de 7.3 milliards de messages par jour) était considéré à l'époque comme préoccupant :

> *« Les dégâts engendrés par le spam commencent à peser sur l'architecture du Net. Ce trafic occupe une grande partie (largeur de bande) des tuyaux qui relient les serveurs et font circuler l'information. ».*

L'article rapportait aussi la phrase d'Eric Allman (développeur en 1981 du premier programme de courrier électronique) déclarant : « *le spam va tuer ce que les Québécois appellent joliment le courriel* ».

6 ans plus tard et en dépit d'une envolée du nombre de spams, le web supporte actuellement allègrement plus de 80% de taux de spam sur un volume colossal de 150 milliards de messages par jour. Malgré cette progression fulgurante, la messagerie électronique est toujours en service et reste un mode de communication fortement populaire, aussi bien auprès des professionnels que des particuliers.

A l'inverse, citons la prévision trop optimiste de Bill Gates qui avait annoncé en 2004 que le spam allait être vaincu dans les deux ans. Les espoirs de l'époque placés dans la technologie « Sender ID » (conçue par Microsoft) visant à authentifier le nom de domaine de l'expéditeur d'un courrier électronique sont rapidement retombés. Après avoir essuyé de nombreux échecs (utilisation par les spammeurs, problème de normalisation avec l'IETF, problème lié au système concurrent DomainKeys, déploiement laborieux, etc.), Sender ID n'est plus considéré comme étant la solution ultime au problème des spams. A ce sujet, Alban Peltier (directeur des services de

communication de MSN France) annonçait déjà en 2005 que « Sender ID n'est qu'un facteur discriminant parmi d'autres » [ZNET01].

Guy Roberts, directeur d'Advert Labs déclarait cette année : « *Il n'est plus question de résoudre ce problème, mais seulement de le gérer* » [GNT04]. Relativisons tout de même cette affirmation pour la replacer dans son contexte (à savoir celui d'une société vivant du spam). Bien qu'il soit certainement impossible de prévoir l'avenir du spam dans le long terme, on peut raisonnablement estimer d'après la situation actuelle que l'objectif de vaincre le spam dans un avenir proche semble de moins en moins atteignable.

Premièrement, trop peu d'efforts sont consacrés à la recherche de solutions préventives. Au lieu de travailler en amont, nous nous trouvons aujourd'hui face à une profusion de solutions anti-spam permettant seulement de rendre ce mal plus acceptable. Cela est bien normal puisque ces solutions sont produites par des sociétés qui vivent et génèrent du profit grâce à l'existence du spam. Sa montée en puissance est même bénéfique pour ces dernières, car elle contraint les utilisateurs à recourir à ce type de produits devenus indispensables. Entre la faible efficacité de « Sender ID », l'impact pratiquement inexistant des poursuites juridiques ainsi que des condamnations et l'abandon du principe visant à rendre l'envoi d'emails payant (en argent ou temps CPU), pas de solution préventive crédible se profile pour l'instant.

Une autre raison concerne le comportement des usagers du web. Une étude de la société Marshal révélait en août 2008 que 29% des 622 internautes sondés avaient déjà acheté des marchandises à la suite d'un spam par email [MARS]. Bien qu'on puisse douter de la représentativité de l'étude (portant sur un faible nombre de contributeurs et menée par un éditeur anti-spam), ce pourcentage semble relativement crédible puisqu'une étude menée en 2004 par le cabinet Forrester Research avait mesuré un taux de 20% sur un panel de 6'000 internautes. Cette demande explique donc aisément la profitabilité de ce marché.

Rappelons d'ailleurs que le spam n'est pas seulement soutenu par les consommateurs. De nombreuses variantes (le phishing par exemple) reposent sur la crédulité des internautes. La démarche n'est pas la même : le consommateur a recours à ce commerce car il y trouve un avantage : par exemple le prix, la discrétion, la possibilité de se procurer des marchandises habituellement interdites, etc. L'internaute victime n'en retire par contre aucun bénéfice. En revanche, tous deux contribuent à soutenir le marché du spam.

Cela permet de comprendre que la faiblesse au niveau humain est double. Même si l'on parvenait à sensibiliser suffisamment les internautes afin qu'ils ne se fassent plus piéger (ce qui est déjà tout à fait improbable au niveau mondial), il faudrait aussi trouver un moyen de gérer le problème posé par ces consommateurs qui achètent en connaissance de cause. Vouloir stopper le spam en modifiant le comportement des internautes semble par conséquent difficilement possible.

Une troisième raison laisse penser que le spam n'est pas encore en danger : l'efficacité grandissante des spammeurs et le coût d'envoi toujours excessivement faible. Comme nous l'avons vu dans la majeure partie de cette étude, les spammeurs sont très inventifs. Même si une partie de leurs techniques ont été contrées efficacement par les solutions anti-spam, d'autres s'avèrent particulièrement récalcitrantes et peu maîtrisées (c'est le cas botnets). De plus, la cadence de renouvellement des techniques leur permet d'avoir une longueur d'avance sur les outils de protection.

Ces arguments montrent que les spams ont encore de beaux jours devant eux.

2. Solutions anti-spam

A défaut de stopper le spam à la racine, les entreprises (les particuliers aussi) sont contraintes de se prémunir contre le spam. Ce chapitre traite donc des solutions techniques défensives. Cela ne signifie pas pour autant que seule l'approche technique compte. En effet, d'autres moyens de contrer le spam reposent sur des mesures organisationnelles ou des bonnes pratiques et sont indispensables : sensibiliser le personnel aux dangers du spam, limiter dans la mesure du possible la publication des adresses sur le web, rester prudent face aux messages et pièces jointes suspectes, garder des systèmes à jour, etc.

2.1 Critères de choix des solutions anti-spam

Les solutions anti-spam sont des outils complexes. Afin d'évaluer leurs capacités de façon pertinente et dans leur globalité, il est important de faire le point sur les critères caractérisant un bon anti-spam [PNEX] [ISN99] [01N02] [IDXL01] [JDN04].

2.1.1 Performance

La performance est la résultante d'un ensemble de caractéristiques tel que la qualité des systèmes de filtrage employés ou l'optimisation de l'application. Elle reflète de façon flagrante le résultat produit et l'atteinte des objectifs fixés, c'est pourquoi elle est primordiale.

2.1.1.1 Qualité du filtrage

Point central de la lutte anti-spam car directement représentatif du résultat atteint, la qualité du filtrage se mesure aisément d'après le nombre de messages légitimes classés comme spams (faux positifs) et le taux de spams non détectés (faux négatifs).

Toute la difficulté est de trouver le juste équilibre entre trop de faux positifs et trop de faux négatifs.

2.1.1.2 Diversité des filtres

La multiplication des techniques de la part des spammeurs impose aux éditeurs anti-spam l'emploi de multiples filtres capables de contrer un large panel de menaces. Un outil contre le spam conçu pour détecter des types d'attaques variées permettra donc de réduire le taux de faux négatifs (parfois au détriment du nombre de faux positifs), mais aussi protéger correctement la messagerie dans le temps (les types de menaces étant généralement cycliques).

2.1.1.3 Rapidité & charge

Cela va de soi, l'utilisation d'un anti-spam a un impact sur la rapidité de traitement des messages et sur la charge du serveur. Ce paramètre insignifiant pour les petites structures est à l'opposé très sensible dans les entreprises traitant un grand nombre de messages. En effet, un traitement trop long ou trop lourd en ressources système peut causer « par accumulation » une surcharge du serveur, pouvant conduire à une interruption de service. Certains anti-spams permettent d'évaluer facilement la vitesse du filtrage en fournissant le nombre de messages traités à la seconde ou le temps CPU consommé par message.

2.1.2 Fonctionnalités

2.1.2.1 Alertes, reporting & statistiques

Remonter les incidents, produire des rapports et des statistiques sur le fonctionnement de l'anti-spam permet d'agir de façon réactive et de s'assurer aisément de la bonne marche de l'anti-spam. Cela permet aussi d'identifier la cause d'un problème (qui pourra être par exemple réglé par la suite au moyen d'une règle de filtrage personnalisée).

2.1.2.2 Quarantaine

Fournir à l'utilisateur un moyen de parcourir rapidement les messages bloqués lui permet de récupérer d'éventuels faux positifs. Non seulement cette fonctionnalité est indispensable pour des entreprises ou départements ne pouvant pas risquer de perdre un message légitime, mais elle contribue grandement à l'acceptation d'une nouvelle solution anti-spam auprès des utilisateurs réticents : leur offrir ce moyen de contrôle manuel est sécurisant.

2.1.2.3 Intégration

Certains logiciels anti-spam sont interfaçables avec d'autres services couramment utilisés en entreprise. Certains prennent par exemple en charge les annuaires Active Directory / LDAP, ce qui permet une gestion facilitée et adaptée des messages à destination de certains groupes d'utilisateurs.

2.1.2.4 Protection contre les virus

La plupart des anti-spam actuels intègrent aussi un anti-virus. Cela facilite la gestion (pas d'interfaçage nécessaire) et coûte dans certains cas moins cher que des solutions séparées.

Il serait d'ailleurs inconcevable actuellement de se protéger des spams et non des virus, puisqu'ils sont étroitement liés (ce qui n'était pas le cas à l'époque, lorsque les spams étaient cantonnés à la vente).

2.1.2.5 Prise en charge de langues diverses

Certaines techniques de filtrage du spam sont dépendantes de la langue utilisée. Recourir à une solution prenant en charges diverses langues offre une protection supplémentaire si les spams venaient à changer de langue. Prenons par exemple le cas des messages rédigés en langue chinoise ayant posé des problèmes de filtrage (écrits sans espaces entre les mots, en sens vertical, etc.).

2.1.3 Flexibilité

Conçu initialement de façon générique, un bon anti-spam doit s'adapter à l'entreprise dans laquelle il est installé.

2.1.3.1 Gestion des règles & personnalisation

Offrir des possibilités de personnalisation des règles de filtrage permet d'adapter au mieux l'anti-spam à l'entreprise. Cette fonctionnalité fondamentale est même indispensable dans certains cas, par exemple lorsque l'entreprise est active dans le domaine pharmaceutique (noms de médicaments couramment utilisés) ou financier (messages relatifs à des crédits, placements, actions).

Un système de gestion des exceptions est aussi très important. Non seulement il permet d'éviter des faux positifs, mais il peut aussi contribuer à l'amélioration des performances, par exemple lors de l'utilisation d'une liste blanche : tous les expéditeurs expressément mentionnés sont dispensés de filtrage.

2.1.3.2 Capacité d'auto-apprentissage

Certains outils dits « intelligents » s'adaptent d'eux-mêmes aux besoins. Lorsqu'ils sont efficaces, ils épargnent aux administrateurs système une part des tâches de maintenance. Il résulte tout de même de cette autonomie un risque de perte de contrôle des administrateurs sur l'anti-spam, en raison du comportement s'adaptant constamment et de façon transparente. Cette intelligence artificielle est parfois aussi la cible des spammeurs qui ont recours à des techniques permettant de la tromper.

2.1.4 Administration

Une solution anti-spam dotée d'une administration efficace et conviviale permettra une meilleure gestion et une économie de temps.

2.1.4.1 Qualité de l'interface et facilité d'utilisation

Toujours plus sophistiqués, les anti-spam ont toujours plus besoin d'une interface claire et facile à prendre en main.

2.1.4.2 Déploiement et mise à jour

La facilité du déploiement et des mises à jour est l'un des facteurs à prendre en compte, car il permet d'alléger les tâches d'administration.

2.1.4.3 Compétences nécessaires

Veiller à choisir une solution adaptée aux connaissances disponibles en interne est primordial. Un anti-spam trop ou pas assez perfectionné conduira à des résultats médiocres, car il pourra être mal maîtrisé ou à l'inverse pas assez performant. L'outil choisi doit être en adéquation avec les compétences.

2.1.5 Architecture

Différentes catégories de solutions existent, applicables à différents niveaux.

2.1.5.1 Niveaux d'applications

Les différents niveaux d'application d'une solution anti-spam offrent chacun leur lot d'avantages et d'inconvénients (ce sujet étant traité plus loin). Il convient à chaque entreprise de retenir la solution la plus adaptée à son cas, ce qui focalise le choix à une catégorie distincte.

2.1.5.2 Infrastructure logicielle

L'infrastructure logicielle installée sur le serveur de messagerie est un critère supplémentaire écartant tous les anti-spam non compatibles.

2.2 Types de solutions

Cette partie aborde les solutions anti-spam selon deux approches. Comme décrit précédemment, il existe différents types de solutions prenant place à des niveaux variés (dans l'architecture réseau). L'objectif est d'expliciter leurs différences, leurs avantages et inconvénients respectifs afin d'aider chaque entreprise à choisir le type de solution le plus adapté à son cas.

Nous verrons ensuite que de nombreuses techniques de filtrage des messages existent. Cela nous permettra de comprendre le fonctionnement interne d'un anti-spam

et d'être par conséquent apte à comparer sur le plan technique des solutions concurrentes.

2.2.1 Niveaux d'application d'une solution anti-spam

Selon le type de solution anti-spam, le traitement est réalisé à différents niveaux du cheminement emprunté par les messages. Il peut intervenir en 4 endroits :

- au niveau du poste client
- au niveau du serveur de messagerie
- au niveau d'une passerelle
- hors de l'entreprise (solution externalisée)

Avant de détailler les avantages et inconvénients de chaque solution, il est important de préciser le type de connaissances détenues par les différents acteurs présents aux différents niveaux [ISN99] :

		Connaissances		
		SMTP/MTA/ anti-spam	**Entreprise**	**Métier**
Acteurs	**Postmaster externe** Profil type : Ingénieur système spécialisé SMTP / MTA / Anti-Spam. Le postmaster FAI travaille pour un ensemble d'entreprises dont il ne connait pas les activités.	Forte	Faible	Faible
	Postmaster dans l'entreprise Profil type : Ingénieur système non spécialisé SMTP/MTA/Anti-Spam. Le postmaster travaille pour l'entreprise, il ne connait pas nécessairement le « métier » des utilisateurs.	Moyenne	Forte	Faible
	Utilisateur Profil type : spécialiste métier.	Faible	Forte	Forte

Source : Rapport ISNet 99 – Septembre 2006 [ISN99]

Il est donc primordial de garder à l'esprit les forces et faiblesses des acteurs rattachés à chaque niveau afin de choisir un point d'application répondant le mieux aux besoins (un besoin nécessitant un filtrage générique sera d'avantage sujet à un traitement externalisé qu'un besoin spécifique à l'entreprise).

Dans certains cas, il est possible d'utiliser plusieurs anti-spam à différents niveaux. On peut par exemple réaliser un premier filtrage de façon générale au niveau du serveur

de messagerie, et laisser à l'utilisateur la possibilité d'affiner ce traitement par lui-même en fonction de ses besoins spécifiques (au moyen d'un logiciel anti-spam installé sur son client de messagerie).

2.2.1.1 Au niveau du poste client

Le filtrage des messages au niveau du poste client est couramment utilisé par les particuliers, car il est adapté à leur infrastructure technique (pas de serveur de messagerie mais utilisation des services d'un ISP), parce qu'il est bon marché, voire gratuit, mais aussi parce qu'il est facile à installer et à gérer. Pour ces mêmes raisons, ce type de solution anti-spam conviendra aussi à de très petites structures formées de quelques postes.

Pour les entreprises de taille supérieure (y compris les PME), l'anti-spam au niveau du poste client n'est pas adapté à plusieurs titres [GFI01] [ZSP] [ITPR01] :

- le déploiement et la maintenance sont réalisés individuellement (une mauvaise efficience en résulte).
- la solution (dans le cas ou elle est payante) multipliée par le nombre de postes peut constituer un lourd investissement.
- l'utilisateur devra être formé à maîtriser cet outil. Il devra ensuite gérer et mettre à jour lui-même ses règles de filtrage, avec plus ou moins de succès (mais il est libre de le personnaliser).
- Les spams sont acheminés jusqu'à leur destination. Ils encombrent donc tous les niveaux de l'infrastructure de messagerie : liaison internet et réseau interne (bande passante), serveur de messagerie et poste client (ressources système).

Il peut néanmoins être utilisé en complément d'une autre solution anti-spam pour répondre à certains besoins spécifiques (à condition bien sûr d'être en mesure de supporter les inconvénients susmentionnés).

2.2.1.2 An niveau du serveur de messagerie

A l'inverse du traitement des spams au niveau du client, le traitement depuis le serveur de messagerie est couramment utilisé en milieu professionnel (pour les sociétés disposant d'un tel serveur en interne). Ses avantages contrastent clairement avec les inconvénients du filtrage au niveau du client [GFI01] [GFI02] [ZSP] [ITPR01] :

- le déploiement et la maintenance sont centralisés.
- la prise en charge d'une grande quantité d'adresses email est généralement moins coûteuse (que celle du filtrage au niveau client).
- le traitement ne requiert pas de paramétrisation de la part de l'utilisateur.
- le spam n'est pas transmis jusqu'au poste client (moins de trafic réseau et économie des ressources en bout de chaîne)

- l'entreprise garde le contrôle total sur la solution anti-spam. Ceci est valable aussi bien pour les tâches de configuration que pour le déploiement contrôlé d'éventuelles mises à jours et correctifs (limiter le risque et évaluer l'impact par des tests).

Comme les autres solutions, le filtrage au niveau du serveur présente aussi des inconvénients [ZSP] :

- le traitement consomme des ressources sur le serveur. Ce dernier doit alors être suffisamment puissant pour assurer le bon fonctionnement du service SMTP et des fonctions anti-spam.
- La bande passante internet reste encombrée par les spams.
- L'anti-spam est adapté au serveur de messagerie et au système d'exploitation utilisé. Une modification de cet environnement peut le rendre incompatible.
- Des ressources humaines formées à l'outil sont nécessaires en interne pour l'installation, l'administration et la maintenance de l'anti-spam.

2.2.1.3 Au niveau d'une passerelle

Le filtrage des messages au moyen d'une passerelle anti-spam (située à l'entrée du réseau, généralement dans une DMZ) offre de nombreux avantages similaires au filtrage depuis le serveur (maintenance centralisée, coût, pas de paramétrisation par l'utilisateur).

Cette solution présente aussi d'autres avantages spécifiques [ITPR01] :

- le filtrage est réalisé en entrée, ce qui épargne la bande passante en interne
- les ressources du serveur de messagerie situé en aval sont économisées (il ne réalise plus de filtrage et ne traite que les messages légitimes)
- le traitement est directement réalisé sur le flux SMTP, ce qui le rend tout à fait indépendant du type de serveur de messagerie et du système d'exploitation utilisé. Une modification de l'infrastructure est donc sans effet sur le traitement des spams.

Les inconvénients d'une telle méthode sont aussi semblables aux solutions installées sur le serveur de messagerie (bande passante internet encombrée, ressources humaines nécessaires à son administration).

Concrètement, le traitement des spams au niveau d'une passerelle est réalisable de deux façons :

- en utilisant un serveur dédié : la solution logicielle prend place sur un serveur consacré à cette tâche de filtrage. Le déploiement est moins facile que pour une appliance, mais le dépannage en cas de panne est rapide (pièces de remplacement à disposition ou serveur de secours prêt à prendre la relève).

- en utilisant un boîtier de filtrage autonome (« appliance ») : l'installation est facilitée mais une panne matérielle est problématique puisqu'elle ne peut être résolue rapidement par l'entreprise (à l'inverse d'un serveur facilement réparable, une appliance est composée de matériel propriétaire). La redondance est aussi très mauvaise, à moins d'investir dans deux boîtiers.

2.2.1.4 Hors de l'entreprise (solution externalisée)

Très différente des autres techniques anti-spam, cette approche consiste à déléguer le traitement des spams à un prestataire externe. Elle offre un certain nombre d'avantages [IDXL02] [ZSP] [LASP] :

- la mise en place est rapide et aisée : une simple modification de l'enregistrement MX du serveur DNS permet de diriger le flux de messages sur le prestataire externe. Une fois traité, ce flux est envoyé sur le serveur de messagerie de l'entreprise
- Très peu de ressources humaines sont nécessaires dans l'entreprise pour maintenir un tel service. La formation est aussi réduite à son strict minimum.
- La bande passante internet consommée auparavant par les spams est économisée (de même que les autres ressources de l'entreprise ; le stockage par exemple)
- Le service de messagerie devient hautement disponible (un crash éventuel du serveur de messagerie de l'entreprise ne cause pas la perte des messages reçus pendant ce laps de temps)
- le serveur de messagerie de l'entreprise est protégé contre diverses attaques (DoS, attaques ciblées, etc.), son adresse IP étant masquée par le service anti-spam

Les inconvénients majeurs d'une solution externalisée sont les suivants [GASP] :

- le traitement externalisé de la messagerie est incompatible avec certaines entreprises ou domaines d'activité qui échangent par ce biais des informations sensibles. Mais comme déclare Robert Eustèbe (DSI d'Arte France) au sujet de leur solution externalisée de gestion des spams : « *Il est clair que lorsque l'on souhaite envoyer une information confidentielle, il ne faut surtout pas le faire par Internet ou alors par le biais de procédés de cryptage* » [JDN05]
- les services externalisés sont moins adaptables aux besoins de l'entreprise que ceux conçus pour fonctionner en interne
- un sentiment de perte de maîtrise peut être ressenti dans l'entreprise

2.2.2 Techniques anti-spam

Cette partie présente les principaux types de filtres permettant le tri de la messagerie.

2.2.2.1 Listes noires & RBL

Une liste noire rassemble des adresses de machines ou domaines bannis (car permettant l'envoi ou la transmission de spams). Une RBL (Realtime Blackhole List)

est une liste maintenue en temps réel (son utilisation étant généralement accessible au public) [AOS].

Il arrive malheureusement que des serveurs soient blacklistés à tort. En fonction de la RBL utilisée, le risque de générer des faux positifs est plus ou moins élevé. Plusieurs différences peuvent expliquer ces disparités [ASTK] :

- différents critères peuvent définir qui est considéré comme spammeur
- collectes différentes des nouvelles entrées de la liste
- procédures de retrait des machines ou domaines listés différentes
- autre type de liste (de relais ouverts, proxy ouverts, spammeurs, etc.)

De façon plus générale, les listes noires sont administrées selon 3 catégories d'organisations [ASTK] :

- les associations à but non lucratif dédiées à la lutte anti-spam
- les administrateurs regroupés pour combattre le spam
- les administrateurs indépendants exploitant une liste pour leur utilisation personnelle mais qui en autorisent l'accès au public.

Prendre en compte ces paramètres permet d'évaluer en partie une RBL. A priori, il est conseillé pour les entreprises sensibles au problème des faux positifs de privilégier les RBL maintenues par les associations, moins sujettes à blacklister par erreur des adresses ou domaines légitimes.

Une étude réalisée entre mi-mars et fin octobre 2004 représente bien l'ampleur des erreurs commises [01N03] : l'organisation « Halte Au Spam » a suivi à cette période 72 grandes organisations françaises (dont une part cotées au CAC 40) afin de contrôler leur présence éventuelle parmi une vingtaine de listes noires. Voici les résultats :

- 38 organisations sur 72 ont été listées à au moins un moment de la période concernée
- l'entité la plus blacklistée est un FAI (présent sur 15 listes)
- la liste noire la plus agressive était australienne, bloquant 14 organisations sur 72
- la réputée liste britannique Spamhaus SBL n'a listé aucune des 72 organisations suivies

Manifestement, un choix scrupuleux des listes utilisées est primordial.

Un autre problème grève lourdement l'efficacité des listes noires : l'envoi de spams à partir d'ordinateurs « zombies ». Blacklister ces machines émettrices de spam n'est pas possible puisque les connexions internet grand public utilisent habituellement des adresses IP allouées de façon dynamique. Par ailleurs, le domaine du FAI ne doit pas

être banni sous peine de pénaliser la totalité des abonnés. Ceci explique d'ailleurs pourquoi l'étude ci-dessus avait relevé qu'un FAI avait été banni auprès de 15 listes.

Efficace auparavant, les listes noires sont de moins en moins performantes face aux méthodes d'envoi récentes. Bruno Rasle (co-auteur d'« Halte Au Spam » annonçait à ce sujet début 2007 que cette technique était désormais dépassée [JDN06].

2.2.2.2 Listes blanches

Par opposition aux listes noires, les listes blanches contiennent tous les expéditeurs de confiance.

Utilisée dans la plupart des cas en complément d'autres techniques, la liste blanche est très appréciée car elle dispense l'anti-spam d'analyser le message. De plus, le risque de faux positif est totalement écarté (pour les expéditeurs spécifiés dans la liste).

En principe, une liste blanche est initialement vide : elle se remplit au fur et à mesure des messages légitimes reçus (ce processus d'apprentissage étant automatisé dans la quasi-totalité des outils).

2.2.2.3 Listes grises

Une liste grise permet de se prémunir du spam par un système de rejet temporaire du message [GREY].

Lorsqu'un message est reçu, le serveur crée un triplet formé de :

- l'adresse IP du serveur émetteur
- l'adresse email de l'expéditeur
- l'adresse email du destinataire

Si ce triplet est déjà connu, le message est acheminé. Sinon, le message est temporairement rejeté (un code de refus temporaire est envoyé au serveur émetteur).

Si le serveur émetteur est légitime, il réexpédiera le message plus tard (un serveur envoyant des spams ne le faisant habituellement pas). Le message est alors accepté (le triplet étant placé en liste blanche). Toutefois, un temps d'attente trop court entre les deux messages cause aussi le refus du deuxième message (ce temps étant paramétrable).

Selon Bruno Rasle, le greylisting est globalement satisfaisant mais ne doit pas être utilisé seul :

> *« C'est une technique efficace. Elle est facile à implémenter et permet en premier niveau, d'écrémer rapidement. Mais elle ne suffit pas. Il faut la compléter par d'autres approches. Le greylisting pose en effet comme postulats que les serveurs de messagerie sont bien configurés et que les PC zombies ne retransmettent pas. C'est une vision un peu optimiste. »* *[JDN06]*

Ajoutons également certains points sensibles relevés par Fabrice Prigent de l'Université de Toulouse 1 dans son retour d'expérience [OSSIR] :

- les services disposant de nombreux serveurs traitant l'envoi de messages (p.ex. Hotmail) risquent d'être régulièrement refoulés puisque le deuxième envoi ne se fait pas forcément avec la même adresse IP d'émetteur (le triplet n'étant par conséquent plus le même). Former le triplet avec une part de l'adresse (les 3 premiers bytes par exemple) résout le problème.
- lorsque plusieurs MX sont utilisés, les triplets doivent être stockés dans une base unique
- certains serveurs ne ré-émettent pas les messages à cause d'une mauvaise interprétation du code d'erreur 450 (échec temporaire) considéré comme code 550 (échec définitif). La seule solution est de les placer en liste blanche.

2.2.2.4 Analyse heuristique

L'analyse heuristique est composée de critères permettant d'examiner l'en-tête et le corps d'un message afin d'y déceler des caractéristiques laissant penser qu'il s'agit ou non d'un spam [SECU]. Il résulte de cette analyse l'établissement d'un score. Si ce dernier dépasse un certain seuil, le message est considéré comme spam.

Un moteur d'analyse heuristique est habituellement composé de plusieurs centaines de critères représentés sous forme d'expressions régulières (la liste exhaustive de ceux utilisés par le projet open-source SpamAssassin est consultable dans la source suivante : [SAS01]). L'expression régulière ci-dessous permet par exemple de détecter le mot « cheap » sous diverses formes : « CheAp », « ¢H€@p », « Çh34p », etc.

```
\b[Cc¢Çç]\W{0,3}[Hh]\W{0,3}[EeÈÉÊËèéêë€3]\W{0,3}[AaÀÁÂÃÄÅàáâãäå4@]\W{0
,3}[Pp]\b
```

D'après les résultats atteints (trop de faux positifs ou trop de faux négatifs), il est possible de rendre le filtrage plus permissif ou plus restrictif par une simple modification du seuil définissant le score à partir duquel un message est considéré comme indésirable.

Le point faible de cette technique est qu'elle nécessite une adaptation constante des critères, afin de parer les nouvelles astuces des spammeurs (soit par des mises à jour automatiques, soit manuellement). Lorsque des critères sont ajoutés manuellement, il est possible d'utiliser des services facilitant l'écriture des expressions régulières [KANO].

Autre point faible, celui de la charge de travail engendrée : elle rend l'analyse problématique lorsque le volume de messages à traiter est important.

2.2.2.5 Filtre sur empreinte (bases collaboratives de spams)

Le filtre sur empreinte fonctionne selon le même principe que les anti-virus et leurs bases de signatures. Comme son nom l'indique, une empreinte est réalisée sur le spam (par une fonction de hachage type MD5 ou SHA), puis elle est stockée dans une base de données. Le terme « base collaborative » désigne l'exploitation d'une même base par différents usagers (cette technique puisant son efficacité lorsqu'elle est utilisée à grande échelle).

Lorsqu'un message est reçu, son hash est systématiquement calculé puis comparé aux entrées de la base. Si une correspondance est trouvée, cela signifie que le message testé est un spam (car identique à celui précédemment identifié comme indésirable). L'un des avantages de cette technique est qu'elle nécessite peu de ressources : un rapide calcul du hash, l'interrogation de la base de données puis une simple comparaison de chaînes de caractères.

Des messages différents peuvent avoir la même empreinte, mais la probabilité que cela arrive est extrêmement faible. Limiter ces « collisions » au maximum est d'ailleurs un critère fondamental à toute bonne fonction de hachage [HASH]. Risquer de produire des faux positifs à cause d'une collision est donc quasiment impossible dans la pratique.

Néanmoins, les filtres sur empreinte sont susceptibles de causer des faux positifs pour une autre raison : Il suffit que le hash d'un mail légitime soit ajouté au filtre pour que tous les usagers de la base trient ce même message comme un spam. Là réside toute l'ambiguïté de ce filtre :

- un nouveau spam détecté doit être ajouté le plus rapidement possible à la base de données pour assurer la meilleure protection possible auprès des autres usagers (donc sans intervention humaine).
- l'ajout d'empreintes à la base doit être réalisé scrupuleusement. Un faux positif ajouté à la base aura un impact décuplé, puisqu'il causera des

faux positifs pour chaque autre destinataire (utilisant la même base et ayant reçu le même message).

En pratique, ce risque est moindre puisqu'il s'applique seulement aux messages légitimes envoyés en masse, l'exemple typique étant les newsletters. La correspondance « classique » entre un expéditeur et un destinataire n'est donc pas menacée.

A l'inverse, le taux de faux négatifs est élevé, raison pour laquelle le filtre sur empreinte doit être utilisé en complément d'autres techniques. Deux raisons sont à l'origine de ces erreurs de filtrage :

- La collection d'empreintes stockées n'est pas exhaustive
- les spammeurs génèrent automatiquement des variantes d'un même spam. Puisque le contenu n'est plus identique, l'empreinte n'est plus la même. Certains anti-spam utilisent toutefois une technique basée sur les « ensembles flous » qui leur permet de reconnaître dans certains cas l'égalité entre deux variantes). Ajoutons également que cette adaptation des spammeurs causée par les filtres à empreinte à des effets néfastes sur la consommation de la bande passante sur internet (un complément d'information à ce sujet est disponible dans la source suivante : [HAS02])

2.2.2.6 Filtres Bayésiens

Le filtre bayésien se base sur des calculs statistiques liés aux mots clés habituellement rencontrés dans les spams ou les messages légitimes. Les prédictions sont réalisées sur la base des expériences passées [LASP].

L'avantage majeur de ce filtre est qu'il s'adapte de lui-même aux besoins. Une entreprise travaillant par exemple dans l'industrie pharmaceutique sera à priori sujette à un taux de faux positifs élevé (certains mails légitimes comportant des noms de médicaments pouvant être confondus avec des spams). L'utilisation d'un filtre bayésien permettra de tenir compte de ce contexte particulier.

Le filtre bayésien est considéré comme efficace et difficile à contourner, mais n'est pas non plus exempt de défauts : non seulement son intelligence artificielle requiert un temps d'apprentissage, mais son efficacité peut être altérée par une technique consistant à créer un « bruit de fond » composé de grandes quantités de textes anodins.

2.2.2.7 Analyse des URL

L'analyse des URL spécifiées dans le corps du message est un bon moyen pour détecter un spam (leur contrôle se fait la plupart du temps au moyen d'une liste noire d'URL).

2.2.2.8 Analyse des pièces jointes

L'analyse des pièces jointes est une technique supplémentaire permettant de détecter les spams, en principe lorsqu'ils véhiculent un malware ou du contenu reconnu comme étant du spam (dans un fichier PDF, GIF, etc.).

2.2.2.9 Contrôle par requête DNS inverse

Partant du principe qu'un serveur de messagerie légitime dispose en règle générale d'une entrée DNS de type PTR (permettant la résolution DNS inverse), un contrôle basé sur l'origine d'un message est possible. Pour cela, on tente de récupérer le nom du serveur émetteur à partir de son adresse IP. Si le serveur DNS ne renvoie pas d'entrée, ou si cette dernière ne correspond pas au nom prétendu, le serveur émetteur est suspect.

Si la requête DNS inverse ne retourne aucun résultat, cela ne veut toutefois pas signifier que le serveur est illégitime, car les entrées PTR ne sont pas obligatoires. Si cette information est utilisée par certains pour tempérer le résultat de l'analyse anti-spam, d'autres refusent catégoriquement tout message provenant d'un serveur ne disposant pas d'entrée PTR (c'est le cas d'AOL) [AOS].

2.2.2.10 Teergrubing

Le teergrubing est une technique originale consistant à maintenir artificiellement une session ouverte sur des connexions suspectes. Concrètement, cela est réalisé en ralentissant l'envoi de lignes de textes prévues initialement par le protocole SMTP pour afficher des messages à l'utilisateur (code de retour 214). Voici un exemple [IKS] :

```
214-This is Sendmail version 8.8.5
214-For more info use "HELP <topic>".
214-To report bugs in the implementation send email to
214-    sendmail-bugs@sendmail.org.
214-For local information send email to Postmaster at your site.
214 End of HELP info
```

Tant que le serveur envoie des lignes de texte et que le code de retour 214 n'est pas suivi par un espace, l'émetteur est contraint d'attendre (ou d'abandonner l'envoi).

En principe, cette technique permet de réduire drastiquement l'efficacité des serveurs d'envoi de spams. Pour y parvenir, il faudrait néanmoins que de nombreux serveurs soient équipés de cette technique.

Par ailleurs, les connexions jugées suspectes à tort ne pourront pas expédier leurs messages avant la fin de ce délai, ce qui peut être particulièrement gênant (l'attente pouvant atteindre plusieurs heures).

Précisons aussi que cette mesure peut être potentiellement détournée de son utilisation normale, ce qui risquerait de faciliter les attaques DoS.

2.3 Etude des solutions disponibles

Cette partie détaille un certain nombre d'anti-spams applicables aux niveaux précédemment décrits. L'objectif est de prendre connaissance des possibilités généralement offertes et des différences entre elles (en dehors de l'aspect financier), et non d'étudier avec exhaustivité l'ensemble des solutions (le marché de l'anti-spam étant passablement atomisé [MIB]).

2.3.1 Solutions logicielles (en interne ou externalisées)

2.3.1.1 GFI MailEssentials

GFI MailEssentials peut être mis en œuvre à différents niveaux : soit directement sur le serveur de messagerie, soit en passerelle (pour les avantages et inconvénients respectifs, se reporter au chapitre « *Niveaux d'application d'une solution anti-spam* »).

Il s'installe sur la plupart des systèmes Windows : Windows Server 2008 (x64), Windows Server 2003 (Standard ou Enterprise, x86 ou x64) ou Windows 2000, et prend en charge Microsoft Exchange (2007, 2003 ou 2000). Installé en tant que passerelle, d'autres serveurs de messagerie sont compatibles (Lotus Notes par exemple) et il peut même être installé sous Windows XP (avec certaines limitations) [GFI03]. Selon l'avis d'un testeur de GFI MailEssentials v12, l'installeur est bien conçu et couvre l'ensemble des prérequis [MTK].

A l'utilisation, cet anti-spam est réputé très efficace. GFI annonce un taux de capture des spams de plus de 98% pour un taux de faux positifs annoncé comme étant le plus faible du marché (mais non précisé !). Les tests semblent confirmer l'excellente efficacité du filtrage.

Techniquement, pour parvenir à de telles performances, une impressionnante quantité de filtres sont implémentés. Citons par exemple l'utilisation de listes noires & RBL, listes blanches, filtre sur empreinte, analyse des URL & pièces jointes, vérification de l'en-tête & mots clés, voire encore l'application d'un filtre bayésien.

Tout message détecté comme spam peut être traité de diverses façons, l'utilisation la plus courante restant son tri dans un dossier directement accessible à l'utilisateur.

GFI MailEssentials ne permet par contre pas de créer des règles personnalisées pour certains groupes ou utilisateurs [MEX01]. De plus, les actions possibles de la part des

utilisateurs sont restreintes et ne leur permettent pas de personnaliser le filtrage. En effet, ils peuvent seulement influer indirectement sur le comportement de l'anti-spam au moyen des actions suivantes :

- Signaler à l'anti-spam les faux positifs
- Signaler à l'anti-spam les faux négatifs
- Ajouter des expéditeurs à la liste blanche d'entreprise
- Ajouter des expéditeurs à la liste noire d'entreprise

Ces actions sont réalisées par l'emploi de dossiers publics accessibles depuis le client de messagerie (voir capture d'écran ci-contre).

Gestion des spams au moyen des dossiers publics (côté utilisateur) [GFI03]

Au niveau de la détection des virus transmis par mail, cet anti-spam devra par contre être associé à GFI MailSecurity, solution complémentaire également réputée pour ses performances. Il est donc important de prendre en compte le coût engendré par l'acquisition de cette deuxième application, qui est quasiment indispensable pour les entreprises ne disposant pas encore d'un outil anti-spam indépendant.

La prise en main de l'application sera quant à elle probablement sans surprise pour une majorité d'administrateurs, puisqu'elle adopte l'interface d'administration classique de Microsoft, la MMC (Microsoft Management Console).

GFI MailEssentials est une solution largement utilisée. Selon l'éditeur, elle compte plus de 80'000 clients. Cette année (ainsi qu'en 2007), elle a remporté la première place du classement *« MSExchange.org Readers' Choice Awards - Exchange Server Anti Spam »* avec 21% des votants, devant les concurrents TrendMicro et Symantec (respectivement 17 et 12%) [MEX02]. Elle bénéficie aussi entre autres de la certification « Checkmark Anti-Spam Premium» (émise par l'organisation West Coast Labs) témoignant des performances offertes (plus d'informations dans la source suivante : [WCL].

2.3.1.2 Trend Micro ScanMail

TrendMicro ScanMail prend place au niveau du serveur de messagerie et existe en différentes versions adaptées à des infrastructures logicielles variées : serveurs Microsoft Windows, Linux, IBM (AIX, i5, z/OS) ou Sun Solaris. Les serveurs de messagerie Microsoft Exchange ou Lotus Domino sont pris en charge.

Contrairement à la solution de GFI nécessitant l'ajout d'un anti-virus, Trend Micro a fait le choix d'intégrer directement l'anti-virus à l'anti-spam (ou plutôt l'inverse, puisque l'anti-spam a été ajouté par la suite).

A l'instar des produits MailEssentials et MailSecurity du concurrent GFI, ScanMail est fortement populaire autant pour son anti-spam que son anti-virus. Au cours des deux dernières années, il a été systématiquement primé lors des *« MSExchange.org Readers' Choice Awards » :*

- 3ème au classement des meilleurs anti-spam pour 2007.
- 2ème au classement des meilleurs anti-spam pour 2008.
- 1er au classement des meilleurs anti-virus (pour messagerie) en 2007 et en 2008.

Malgré ces résultats prometteurs, très peu d'informations sont disponibles sur cet anti-spam : non seulement les tests et avis sur le produit sont anciens et peu nombreux, mais les informations fournies par l'éditeur sont particulièrement succinctes : les filtres implémentés, les autres informations techniques ou encore les renseignements sur les fonctionnalités sont peu détaillées.

Trend Micro ScanMail bénéficie aussi de la certification Checkmark (le dernier test date de juillet 2008). Malheureusement, on n'en saura pas d'avantage puisque le rapport n'est pas disponible (contrairement à *« InterScan Messaging Security Suite »*, anti-spam agissant au niveau de la passerelle et aussi édité par Trend Micro).

Voici néanmoins les principales caractéristiques de ScanMail (trouvées notamment dans le manuel) [TDM01] [TDM02] :

- Les spams sont détectés par les techniques suivantes (liste non exhaustive) :
  - liste noire et liste blanche configurées par l'administrateur
  - liste blanche personnelle configurée par l'utilisateur final (pas d'information sur une éventuelle liste noire)
  - apprentissage automatique
  - analyse heuristique
  - filtre sur empreinte
  - analyse des URL
- le seuil auquel un message est classé comme spam est adaptable et peut être fixé indépendamment d'après différents types de contenus (finance, santé, etc.)
- Un spam détecté peut être traité de différentes façons :
  - supprimé
  - mis dans la *« End User Quarantine »* (EUQ). Il s'agit d'une quarantaine côté serveur accessible par l'utilisateur final via une

interface web. EUQ est un composant optionnel (la fonction associée étant bien entendu inaccessible si EUQ n'est pas installé).

    - taggé dans l'en-tête du message (le client de messagerie utilisant ce tag pour classer le spam dans un dossier approprié).
- l'administration se fait depuis une interface web.

Un test grandeur nature sera certainement à même de mieux cerner le produit (comme beaucoup d'autres anti-spam, ScanMail est disponible en version d'évaluation). Si son efficacité s'avère satisfaisante, de nombreuses entreprises y trouveront leur compte, d'autant plus qu'une étude d'Osterman Research a conclu en février 2008 que cet anti-spam était moins coûteux que d'autres produits concurrents (non pas à l'achat, mais lors de son exploitation) [SYSC].

Une attention toute particulière devra cependant être portée sur sa performance et sur la qualité des rapports générés, ces points faibles ayant été mis en évidence lors des tests réalisés sur une version antérieure (6.2) [SCM01].

2.3.1.3 SpamAssassin

SpamAssassin est une solution anti-spam open-source développée par l'Apache Software Foundation (éditrice du serveur web Apache). Fortement adaptable, Spam Assassin peut être installé sur divers serveurs de messagerie, tant sur Linux (cas le plus courant) que sur Windows, voir même sur Mac OS X [SAS02].

Le tri est principalement réalisé au moyen des tests suivants [SAS03] :

- contrôle de l'en-tête et du corps du message (analyse heuristique composée de règles de base et personnalisées)
- filtrage bayésien
- listes blanches et noires automatiques et manuelles
- utilisation de bases collaboratives de spams (filtre sur empreinte)
- utilisation de RBL
- analyse du jeu de caractères utilisé

La décision d'exclure ou non un message est prise en fonction d'un score calculé. Si ce dernier dépasse un seuil limite (configurable), le message est traité en tant que spam.

A la différence de nombreux anti-spams, SpamAssassin n'intègre aucune protection anti-virus nativement, mais il peut être interfacé à un programme tiers dédié à cette tâche.

Comme le témoignent les nombreux forums dédiés à l'open-source, SpamAssassin est fortement populaire en raison de sa gratuité et de la communauté supportant activement le projet. Cependant, cette solution est nettement plus difficile à installer que la plupart des autres anti-spams et la qualité du filtrage n'est habituellement pas optimale avec la configuration par défaut. Un temps d'apprentissage ainsi qu'une bonne administration seront donc nécessaires pour révéler tout le potentiel de SpamAssassin.

Indispensable pour le déploiement et la configuration initiale, cet anti-spam requiert aussi une gestion adéquate dans le temps. Cela est particulièrement vrai puisque les règles utilisées pour le filtrage des messages ne sont pas mises à jour automatiquement. Pour bénéficier des règles actuelles, c'est l'anti-spam entier qui devra être mis à jour [HSC].

Très différent des produits commerciaux, SpamAssassin conviendra à des entreprises disposant des ressources adaptées, aussi bien au niveau de leur disponibilité que des qualifications. Attention également à ne pas se laisser attirer par la gratuité de l'application : indubitablement, l'administration régulière du système a un coût caché (mais bien réel) ne devant pas être sous-estimé. Enfin, SpamAssassin est réputé pour consommer beaucoup de ressources. Sa mise en œuvre sera probablement plus délicate dans les entreprises traitant de grands volumes de messages.

2.3.1.4 MailInBlack-Asp

Le fonctionnement de MailInBlack diffère des autres produits. Au lieu d'adapter constamment les techniques de filtrage aux évolutions du spam, cette solution utilise des mécanismes relativement simples et durables.

Le principe sur lequel se base MailInBlack est le « test de Turing » (imaginé dans les années 50 par Alan Mathison Turing). Si un testeur (humain) dialogue avec un correspondant distant sans pouvoir clairement déterminer s'il s'agit d'une machine ou d'un autre humain, le test est réussi.

MailInBlack utilise donc ce test pour différencier les messages provenant d'un individu de ceux émis de façon automatisée. Bien entendu, cela est possible car les systèmes d'envois massifs de messages ne passent pas le test avec succès. En pratique, le système procède de la façon suivante :

- lorsqu'un expéditeur envoie un message sur une adresse email de l'entreprise, le système vérifie qu'il est présent dans une liste blanche. S'il s'y trouve déjà, cela signifie qu'il est un expéditeur légitime. Son

message est donc délivré directement. Sinon, le système lui demande de répondre à un Captcha.

- Si l'expéditeur a répondu correctement au Captcha, il est légitime donc ajouté en liste blanche. Son message est transmis au destinataire.
- Les futurs envois de ce même expéditeur seront délivrés directement au destinataire.

L'avantage principal d'une telle solution est son efficacité. En effet, le taux de faux négatifs est de 0% (sauf cas exceptionnel, par exemple lorsque l'adresse d'un expéditeur approuvé est utilisée à mauvais escient ou si le spammeur parvient à passer le test). Le taux de faux positifs est aussi de 0% pour autant que le test parvienne correctement à l'expéditeur, et que ce dernier le réussisse avec succès.

Un autre avantage concerne son administration réduite : pas de filtres complexes à configurer, pas de score limite à fixer (puisque la décision prise est strictement binaire), et pas besoin d'adapter son anti-spam au cours du temps (les spammeurs ne passent généralement pas ces tests, soit pour des raisons techniques, soit parce qu'ils ne prennent pas la peine d'y répondre). Cet argument se voit renforcé par MailInBlack-Asp, la version externalisée, puisqu'elle réduit au maximum le déploiement et les tâches habituelles de maintenance.

L'inconvénient majeur de MailInBlack est la gène qu'il occasionne. Suivant le domaine d'activité, cette solution peut être inadaptée voire incomprise de l'expéditeur.

Une autre conséquence de MailInBlack est qu'il augmente d'avantage le volume de messages transmis, mais aussi qu'il peut submerger un service distant déjà victime des spammeurs. C'est par exemple le cas des services de messagerie gratuits exploités par les spammeurs pour l'envoi de messages. Non seulement ces services sont pénalisés par l'accroissement du trafic causé par les messages sortants, mais aussi par les demandes de validation (tests de Turing).

2.3.2 Solutions matérielles

2.3.2.1 IronPort Email Security Appliances

IronPort (entreprise détenue par Cisco depuis 2007) propose une gamme d'appliances dédiées à la protection de la messagerie. Les 6 modèles proposés couvrent un large éventail de besoins pouvant aller de la PME au grand ISP. Le fonctionnement général est toutefois commun à ces différents modèles.

La détection des spams est réalisée en deux temps. Un premier filtre par réputation permet d'éliminer plus de 80% du spam entrant. Pour maintenir ce filtre, IronPort

dispose d'un vaste réseau nommé « SenderBase ». Ce dernier analyse 25% du traffic mondial des emails à l'aide de 75'000 entreprises participantes et utilise plus de 110 paramètres différents pour définir la réputation d'un expéditeur [01N04]. Ce filtrage est un excellent premier obstacle au spam : ses bonnes performances permettent d'alléger considérablement la charge, les processus de détection plus lourds tel que l'analyse du contenu étant ainsi épargnés.

Les 20% de spams résiduels sont traités par un ensemble de filtres complémentaires (sur l'en-tête, le contenu, les URL, les pièces jointes, etc.). Ces derniers n'ont pas été developpés par IronPort, il s'agit de ceux de Symantec BrightMail.

De même que l'anti-spam de Trend Micro, les appliances IronPort disposent aussi d'un anti-virus dont l'architecture générale est identique à l'anti-spam : un premier niveau de filtrage conçu par IronPort s'appuie sur les analyses du réseau SenderBase, tandis qu'un deuxième provient d'une entreprise externe, en l'occurrence de chez Sophos.

Une étude publiée en 2007 par l'entreprise de consulting Opus One a révélé les taux suivants mesurés en pratique [OPUS] :

- 95.03% des spams ont été détectés, résultat pouvant être qualifié de relativement moyen.
- 0.14% de faux positifs. Très bon résultat, mais tout de même bien loin des promesses annonçant un taux record de faux-positifs de l'ordre d'un message sur 1 million (soit maximum 0.0001% de faux positifs !).
- 51.80% des spams ont été détectés par le filtre par réputation. Là aussi, les résultats sont nettement moins bons que ceux annoncés (plus de 80%).
- seulement 0.02% des faux positifs ont été causés par le filtre par réputation.

Sans entrer dans les détails, précisons que les tests, récompenses et avis des utilisateurs sur les produits IronPort sont généralement très positifs (mais les tarifs sont relativement élevés) [SCM02] [SAGE] [IWOR].

Cette solution sera adaptée d'une manière générale aux besoins suivants :

- besoin justifiant le filtrage de la messagerie au niveau de la passerelle (avec les avantages et inconvénients d'une telle installation)
- nécessité de limiter au maximum les faux positifs (à condition peut-être de tolérer un taux de faux négatifs légèrement plus élevé que ceux atteints par des produits concurrents). Les utilisateurs pourront naturellement contrôler ces quelques faux positifs via une zone de quarantaine.
- limiter (dans la mesure du possible) les tâches d'administration et de maintenance sans recourir pour autant à une solution externalisée risquant d'entraîner une perte de maîtrise ou des problèmes de

confidentialité des informations. L'argument récurrent d'IronPort est d'ailleurs *« Just plug them in-spam and viruses go away »*.

- traiter de grandes quantités de messages. Non seulement les boîtiers de filtrage IronPort déchargent le serveur de messagerie (caractéristique classique des solutions installées en amont), mais ils sont réputés très performants :
    - comme décrit précédemment, le premier niveau de filtrage décharge rapidement une grande quantité de messages qui ne seront donc pas traités par le second niveau, dont l'exécution est plus lourde.
    - Le système d'exploitation utilisé (AsyncOS) est performant car dédié à ces tâches de filtrage (il est également épaulé par un système de fichiers propriétaire « AsyncFS ») [CORT]. Il est de surcroît dérivé de FreeBSD, système éprouvé pour ses performances et sa sécurité.
    - au niveau matériel, ces appliances embarquent un ou plusieurs processeurs multi-cores capables de paralléliser les traitements.

2.3.2.2 Sophos Email Appliances

Sophos commercialise deux appliances anti-spam : l'ES1000 et l'ES4000. Ces deux versions se différencient d'après leur configuration matérielle, celle de l'ES4000 étant nettement meilleure [SOPH02] :

- Bi-processeur Intel Xeon au lieu d'un Intel Celeron D
- 2GB de RAM au lieu d'1GB
- 2 disques durs SCSI hot swappables en RAID1 au lieu d'un seul en SATA
- Alimentation redondante (l'autre ne l'étant pas)

Les différences de ces deux configurations influencent deux facteurs (en dehors des considérations financières) : alors que le premier est, sans surprise, les performances (l'ES4000 peut traiter 80'000 messages par heure au lieu de 20'000 pour l'ES1000), le deuxième est bien plus pernicieux, puisqu'il impacte la fiabilité du système. A l'évidence, un crash du disque non répliqué ou une défaillance de l'alimentation électrique causeront de graves troubles sur l'ES1000 (interruption du service avec probablement perte d'informations) tandis que l'ES4000 restera pleinement opérationnel. Cette faiblesse n'est donc pas à négliger, à plus forte raison car de telles pannes ne sont pas rares (une analyse menée par Google sur sa propre infrastructure matérielle a révélé que 8% de leurs disques durs étaient tombés en panne dans les 3 ans [JDN07]).

Au niveau des possibilités, Sophos se différencie de la concurrence par leur concept appelé « appliances administrées ». Il s'agit d'une appliance classique à laquelle on a

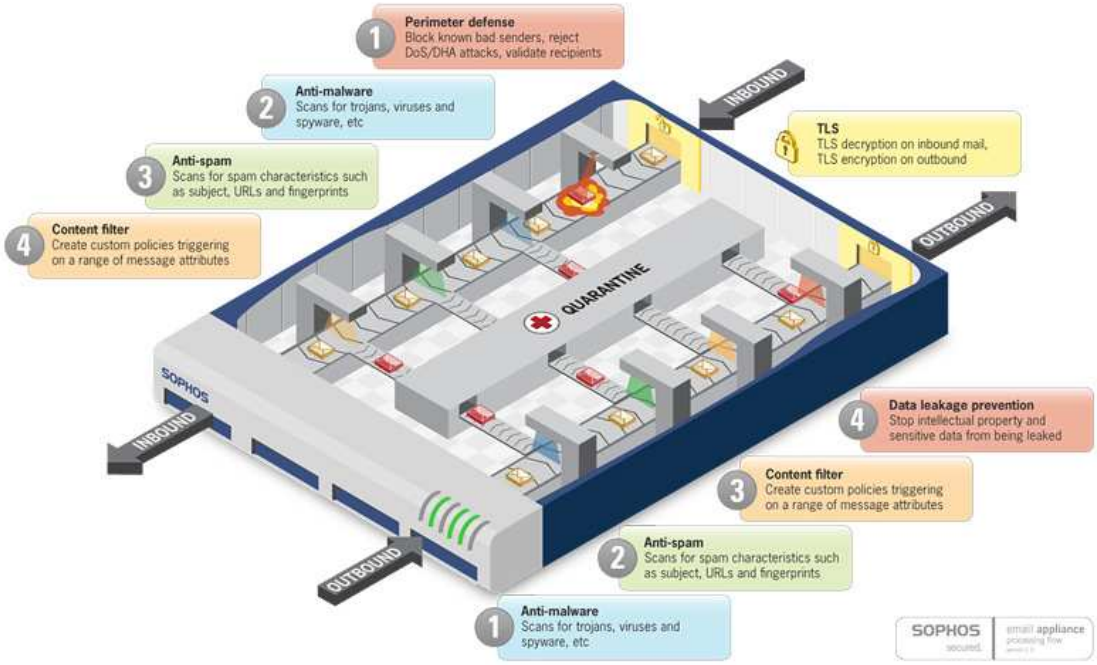
ajouté des fonctionnalités de surveillance et de gestion distante accompagnées d'un service de surveillance continue assuré par Sophos.

Cette variante située à mi-chemin entre les appliances classiques et les solutions externalisées est un bon compromis pour les entreprises ne disposant pas des ressources nécessaires pour gérer complètement une solution anti-spam en interne. Par rapport aux solutions externalisées, une appliance administrée procure au client une meilleure liberté d'action. L'offre de Sophos n'est d'ailleurs pas conçue pour prendre en charge intégralement les tâches d'administration, mais plutôt pour fournir aux clients une protection contre les défaillances, cette maintenance permanente étant capable de détecter et de prendre en charge rapidement les incidents qui surviennent.

Au même titre qu'IronPort, Sophos dispose aussi d'un premier niveau de filtrage efficace et performant permettant d'éliminer une grande quantité de spams et d'alléger drastiquement la charge du système, à la différence qu'il n'utilise pas de filtre par réputation mais un système propriétaire nommé *« Sender Genotype »*. Ce filtre a été conçu pour contrer les spams émis depuis les botnets pour lesquels le filtrage par réputation basé sur les adresses IP montre ses limites (problème de l'allocation dynamique des IP). Sender Genotype a donc l'ambitieuse tâche de savoir reconnaître les connexions en provenance d'un botnet, toute connexion détectée comme telle étant immédiatement interrompue [GSMO2]. Les techniques utilisées concrètement pour accomplir cette détection ne sont pas précisées par Sophos, mais on peut vraisemblablement comprendre que révéler le fonctionnement de ce filtre risquerait de le rendre inefficace dans le temps ou pourrait avantager les sociétés concurrentes.

Le traitement des autres spams non détectés par Sender Genotype passeront par différents filtres, certains permettant aussi d'abandonner les nouveaux spams dès leur connexion (notamment par réputation IP), tandis que différents niveaux de filtrages plus classiques déplaceront les messages détectés comme spams dans une zone de quarantaine (heuristique, empreinte des messages et pièces jointes, détection d'URL, etc.). Une analyse anti-virus (incluant toutes sortes de malwares) a aussi lieu.

Pour récapituler, le schéma ci-dessous illustre clairement la chronologie du filtrage pour les mails entrants et sortants :



Source : Sophos [SOPH03]

Un autre système appelé *« SXL »* (Sophos eXtensible Lists) fournit aux clients des mises à jour toutes les 5 minutes. Il permet aussi d'alléger la taille des mises à jour en laissant certaines informations moins fréquemment utilisées accessibles si besoin à distance.

Un test réalisé sur l'ES1000 (version adaptée aux PME) révèle les constatations suivantes [ITPR02] :

- Le service de surveillance à distance a bien réagi en fonction des incidents survenus (certains ayant été provoqués intentionnellement).
- Les mises à jour déclenchées toutes les 5 minutes (SXL) n'ont pas pu êtres réalisées de temps en temps, mais le service de surveillance a émis correctement une alerte.
- L'efficacité du filtrage est bonne. Un premier test réalisé sur 632 messages dont 244 spams annonce un taux de détection de plus de 97% et aucun faux positif (système réglé sur la mise en quarantaine de tous les messages dont le score était moyen ou élevé).
- Le spam peut être traité de diverses façons : jeté, mis en quarantaine (accessible aux utilisateurs via une interface web), taggé ou redirigé.
- Le déploiement et l'administration sont aisés.
- L'interface web est intuitive et agréable à utiliser au quotidien.

- L’interface web dispose d’un tableau de bord clair de l’état du système, et les possibilités offertes par le reporting sont bonnes (mais il n’est possible d’exporter des données qu’au format CSV).
- Des lenteurs occasionnelles de l’interface d’administration ont lieu.
- La configuration matérielle de l’appliance est jugée pas assez performante en regard du prix.

Un autre test réalisé fin 2007 a comparé 3 appliances anti-spam des entreprises Sophos, IronPort et ClearSwift [SOPH04]. L’ES1000 est déclaré grand vainqueur et un taux mirobolant d’interceptions est annoncé : 99.4% des spams ont été filtrés (sur 10'000 messages approximativement). Mais en y regardant de plus près, on peut lire en bas du rapport le texte suivant :

> *« Ce rapport comparatif, mené indépendamment par evisionIT Labs, a été sponsorisé par Sophos. evisionIT Labs s’attache à proposer une analyse objective et impartiale de chaque produit d’après des tests réalisés dans ses laboratoires et à fournir à chaque entreprise dont les produits sont testés la possibilité d’y participer en intervenant sur le plan de test et les résultats d’evisionIT Labs. »*

On peut donc tout de même douter de l’impartialité de l’étude, à plus forte raison parce que le taux annoncé d’interception des spams est non seulement très élevé mais aussi parce qu’il ne correspond pas aux résultats du test précédemment décrit (en revanche, il correspond aux chiffres avancés par Sophos sur son site web).

Bien qu’on ne puisse pas se prononcer clairement sur la meilleure solution des trois (chacune présentant assurément son lot d’avantages et d’inconvénients), cette appliance présente néanmoins d’indéniables qualités qui pourront convenir à nombre d’entreprises. L’approche de Sophos consistant à conserver le traitement des spams en interne tout en assurant un support en externe est une idée novatrice qui offre une alternative pour les sociétés ne pouvant pas assurer correctement la maintenance permanente d’un anti-spam et pour lesquelles le choix d’une solution externalisée ne convient pas.

3. Choix d'une solution et étapes de mise en place

En raison de l'importance qu'elle occupe en milieu professionnel, la messagerie est un service essentiel au bon fonctionnement d'une entreprise. Toute action réalisée à son niveau doit donc être réalisée avec une certaine prudence.

Pour cette raison, choisir et mettre en place un anti-spam est un exercice qui nécessite l'application rigoureuse d'un plan d'action clairement établi. Cette démarche est importante, voire indispensable, car elle fournit un cadre tout au long du processus, ce qui permet de prévenir un certain nombre de problèmes inhérents à un tel projet (perturbations, interruptions de service, réticences ou refus de la solution par les utilisateurs, etc.). Si un tel processus n'est pas géré correctement, il peut aller jusqu'à causer l'échec du projet tout entier.

Cette partie présente donc les étapes composant un projet anti-spam. Il va de soit qu'il s'agit d'un squelette général appelé à être adapté en fonction du contexte. A ce titre, certaines tâches présentées ci-après ont par exemple été dissociées pour une meilleure clarté, ce qui n'empêche pas forcément leur regroupement en pratique.

3.1 Phase 1 : Etude préalable

3.1.1 Situation actuelle, besoins, contraintes et objectifs

Analyser la situation actuelle constitue la base du projet [AFR]. Durant cette étape, l'étude sera centrée sur un certain nombre d'éléments fondamentaux, en particulier :

- le nombre d'adresses emails gérées
- le volume de messages quotidiennement traités
- l'infrastructure (environnement matériel et logiciel)
- les solutions anti-spam actuellement en place (si existantes), ainsi que leurs avantages et inconvénients.
- les ressources humaines à disposition (appelées à gérer la solution anti-spam), tant au niveau de la disponibilité que des compétences
- les critiques formulées par les utilisateurs

Toute la difficulté réside dans le niveau de granularité de l'étude. Cette dernière doit être relativement détaillée pour couvrir les différents aspects de la messagerie, tout en restant synthétique, ce qui permet d'avoir une bonne vue d'ensemble. Si toutefois les personnes en charge du projet connaissent déjà passablement bien l'infrastructure en place, cette étape peut s'avérer superflue.

En s'appuyant sur les éléments mis en évidence par l'analyse de l'existant, les besoins et contraintes sont ensuite formalisés, de même que les objectifs poursuivis. Ces derniers doivent être explicites, atteignables et mesurables [ISN99].

3.1.2 Détermination du niveau d'application

Comme nous l'avons vu précédemment, les caractéristiques des différents niveaux d'application d'une solution anti-spam diffèrent. Choisir le niveau le plus adapté se fera en fonction des besoins et contraintes définies lors de l'étape précédente (par exemple besoin d'un filtrage flexible, contraintes de confidentialité ou contraintes budgétaires, etc.).

Dans certains cas, il est possible de recourir à un filtrage multi-niveaux. Il faut tout de même veiller aux éventuels problèmes qui peuvent être causés par une telle solution (risques d'une gestion et maintenance inefficiente, quarantaines ou rapports multiples, augmentation de la complexité auprès des utilisateurs, etc.).

3.1.3 Etude de l'offre et sélection de solutions concurrentes

En partant des offres disponibles pour le niveau précédemment défini, l'objectif de cette étape est de former une sélection des meilleures solutions capables de répondre aux besoins tout en respectant les contraintes. Ces solutions seront ensuite testées durant la phase 2 du projet.

Il n'y a pas réellement de règle concernant le nombre d'anti-spams à sélectionner, cela est à définir en tenant compte du fait qu'un nombre élevé de solutions retenues (donc testées) permettra de réaliser un benchmark très représentatif des possibilités offertes entre produits concurrents, mais prendra bien entendu beaucoup plus de temps (et donc plus de ressources mobilisées). D'autres effets pernicieux ne sont pas exclus si la période de test s'éternise, en particulier la possible démotivation des équipes impliquées.

Pour ces raisons, il est vraisemblablement judicieux de filtrer au maximum les solutions sur la base de leurs spécifications ainsi que sur les éventuels tests et retours d'utilisateurs disponibles. La deuxième phase (les tests) doit être vue comme un outil permettant de contrôler en pratique les possibilités offertes par chaque anti-spam, mais aussi de les départager. Il est également possible de ne sélectionner qu'un seul anti-spam, la phase de test étant alors utilisée pour contrôler que les objectifs sont atteints (on perd donc l'aspect comparatif).

3.2 Phase 2 : Tests

Tester un anti-spam permet de contrôler un certain nombre d'éléments [DRM] :

- vérifier que la messagerie est toujours opérationnelle (l'anti-spam étant placé sur le chemin emprunté par les messages)
- contrôler la qualité du filtrage
- mesurer la charge
- tester les procédures opérationnelles (mise à jour, sauvegarde, redémarrage, etc.)
- étudier le comportement des utilisateurs face à la nouvelle solution (facilité de prise en main, réclamations, etc.)

3.2.1 Planification & information

Planifier le déroulement de la phase de test et informer les acteurs impliqués sont des tâches essentielles qui permettent de fixer la chronologie des étapes, de déterminer leurs durées respectives ou encore de fixer les responsabilités de chaque intervenant. Cela permet aussi de s'assurer que chaque employé investi dans le projet sera disponible au moment voulu [DRM].

3.2.2 Création d'un groupe de test

Les avis divergent à propos du déploiement de la solution testée. Tandis que certains conseillent d'appliquer l'anti-spam testé sur tous les utilisateurs de l'entreprise [MFR], d'autres recommandent une démarche très différente : restreindre l'application de la solution à un groupe de test formé pour l'occasion.

Si la première approche permet d'apprécier les possibilités de l'anti-spam dans des conditions identiques à celles rencontrées en production, elle présente tout de même un inconvénient majeur : celui du risque. En effet, de multiples incidents peuvent impacter la messagerie, par exemple si la solution testée ne donne pas satisfaction ou si elle n'est pas configurée correctement. D'autre part, certains essais plus risqués peuvent être entravés par la responsabilité d'assurer impérativement le fonctionnement sans accroc du service de messagerie dans son ensemble.

A l'inverse, la deuxième approche est beaucoup plus prudente puisque les défaillances susceptibles de survenir impacteront seulement un groupe restreint d'utilisateurs conscients des incidents possibles et ayant accepté de participer au test. Malgré le fait que cette méthode soit moins proche des conditions réelles, il est généralement possible d'extrapoler les résultats à l'ensemble de l'entreprise (pour estimer la charge occasionnée par exemple). Pour ces raisons, la formation d'un groupe de test paraît

être la meilleure solution (les étapes décrites ci-après sont donc calquées sur cette façon de procéder).

Les utilisateurs consentants sélectionnés pour former le groupe de test doivent être dans la mesure du possible [DRM] :

- curieux et persévérants
- non réfractaires au changement
- impliqués au projet
- conscients de leur rôle et de l'importance des tests
- capables de fournir un feed-back constructif (positif ou négatif)
- en mesure de consacrer suffisamment de temps pour participer correctement au projet
- discrets face aux problèmes rencontrés lors des tests car conscients du tort que cela pourrait causer au projet
- capables de « vendre » la solution aux collègues

3.2.3 Formation du groupe de test

La formation des testeurs remplit un double objectif :

- les préparer à l'utilisation de la nouvelle solution
- tester l'efficacité de la formation (et la rectifier si besoin avant de la donner à tous les employés)

3.2.4 Exécution du test

Pour permettre une évaluation représentative des anti-spam sélectionnés, chaque solution doit être testée à tour de rôle et non simultanément. La période de test recommandée est d'environ 2 semaines par anti-spam [MFR].

Naturellement, chaque solution testée sera soumise aux mêmes critères d'évaluation. Ces derniers auront pour tâche de contrôler l'atteinte des objectifs et devront être définis avant le début des tests.

Concrètement, les produits testés sont généralement mis gratuitement à disposition par les éditeurs sous forme de versions d'évaluation.

Durant l'exécution du test, les utilisateurs vont devoir mettre à profit la formation qui leur a été donnée, non seulement pour savoir utiliser l'anti-spam, mais aussi pour rectifier les erreurs de filtrage (faux positifs et faux négatifs). Cette dernière tâche est primordiale pour les raisons suivantes :

- elle permet d'entraîner l'anti-spam (à condition qu'il dispose de mécanismes d'apprentissage tel que l'emploi d'un filtre bayésien)

- elle permet de mesurer l'efficacité du filtrage, puisque le nombre de faux positifs et de faux négatifs n'est pas quantifiable sans intervention humaine

3.2.5 Bilan

En s'appuyant sur les résultats des tests, la solution la plus adaptée est choisie en vue de son déploiement.

La formation est quant à elle ajustée, notamment grâce aux critiques, questions et éventuelles suggestions formulées par le groupe de test.

3.3 Phase 3 : Déploiement

3.3.1 Information auprès des utilisateurs & formation

Modifier les outils informatiques et les méthodes de travail est parfois mal perçu par nombre d'employés. Résistants au changement car inquiets de l'impact de ces modifications sur leurs tâches quotidiennes ou simplement à cause d'une mauvaise compréhension de la finalité de la démarche, ces employés peuvent conduire le projet anti-spam à l'échec. Les informer à l'avance et de façon suffisante avant de procéder au déploiement de la solution anti-spam est donc une tâche à ne pas négliger, car elle contribue à une meilleure acceptation de ce changement. Des conférences seront donc organisées durant lesquelles les employés seront informés de la nécessité d'un tel projet, des objectifs poursuivis, des répercussions sur leur travail, etc. Ils auront aussi l'occasion de s'exprimer librement sur le sujet et de poser des questions.

Comme pour l'équipe de test, l'ensemble des utilisateurs suivra ensuite une formation qui leur permettra d'apprendre à utiliser correctement le nouvel anti-spam. Une fois les employés familiarisés à ce nouvel outil, le déploiement se fera sans surprise, ce qui contribuera à augmenter leur confiance et leur satisfaction. La charge du helpdesk sera aussi allégée, il pourra alors traiter efficacement d'éventuels imprévus.

3.3.2 Mise en production

Une fois l'anti-spam mis en production, les équipes devront contrôler son bon fonctionnement et se tiendront prêtes à réaliser, si besoin, d'éventuels ajustements. Le support informatique quant à lui sera à l'écoute des utilisateurs et collaborera avec l'équipe messagerie.

4. Cas pratique : Paléo

Paléo, association organisatrice du Paléo Festival ayant lieu chaque année à Nyon est composée de 44 employés en période hors festival et de 60 employés pendant le festival.

Comme la quasi-totalité des entreprises, la messagerie est un outil essentiel à la réalisation de nombreuses tâches. Confrontée (sans surprise) aux spams, Paléo utilisait jusqu'à présent une solution externalisée auprès d'un prestataire de services suisse.

Insatisfaite par les possibilités offertes par ce système de filtrage principalement en raison de limitations au niveau de la paramétrisation et de la gestion déléguée par utilisateur, Paléo a récemment changé de solution anti-spam.

Avant de traiter du nouvel anti-spam choisi, il est important de faire le point sur la situation et les besoins de Paléo dans le but de mieux cerner quel type de solution est le plus approprié.

La situation générale de l'infrastructure en place est la suivante :

- La messagerie comporte 80 adresses email et gère quotidiennement un volume d'environ 3500 messages (en comptant aussi les spams).
- Le serveur de messagerie utilisé est Microsoft Exchange Server 2003 (installé sur Microsoft Windows Server 2003)

  Voici l'occupation moyenne des ressources :
  - CPU : 11%
  - Mémoire vive : 52%
  - Disque dur : 46%
- Les postes clients fonctionnent sous Microsoft Windows XP Professionnel et utilisent le client de messagerie Microsoft Office Outlook 2007

Voici les principaux besoins et contraintes :

- Les utilisateurs doivent avoir la possibilité d'accéder à une quarantaine leur permettant de récupérer les éventuels faux positifs et doivent pouvoir modifier individuellement certains paramètres de l'anti-spam.
- Les ressources humaines disponibles ne permettent pas la prise en charge d'une solution anti-spam intégralement gérée en interne
- L'utilisation d'un service externalisé ne pose pas de problème de confidentialité des données traitées à condition que des clauses claires (et acceptables) soient prévues dans le contrat.

D'un point de vue technique, la mise en place d'un anti-spam sur le serveur de messagerie aurait donc été envisageable en raison des ressources matérielles

disponibles et de la quantité relativement restreinte de messages à traiter. Rapatrier ces 3500 messages quotidiens n'aurait pas pesé non plus bien lourd sur la bande passante internet. En revanche, comme décrit précédemment, les ressources humaines disponibles ne permettent pas l'utilisation d'une solution anti-spam interne à l'entreprise. Pour cette raison, une solution anti-spam externalisée convient en raison de son avantage premier qui est justement la délégation des tâches de configuration et de maintenance qui n'ont, dès lors, plus besoin d'être assurées par l'entreprise.

Répondant aux besoins, la solution externalisée MailCleaner Hosted Services a été choisie. Voici un aperçu de ses possibilités :

- Une trentaine de contrôles permettent de déterminer si le message analysé est un spam. L'efficacité du filtre annoncée est d'environ 99%.
- Les virus et autres contenus malveillants sont aussi filtrés
- Chaque utilisateur dispose d'une zone personnelle accessible via une interface web. Elle est séparée en 4 sections :
    - Configuration (action à entreprendre lorsqu'un spam est détecté, possibilité de planifier l'envoi automatique d'un rapport, gestion de listes d'avertissement et listes blanches, etc.)
    - Quarantaine (consulter ou libérer un message filtré, signaler un faux positif, etc.)
    - Statistiques
    - Aide
- Si l'utilisateur dispose de plusieurs adresses emails, il peut accéder aux différentes options à partir d'une seule interface de gestion
- L'utilisateur peut signaler tout faux négatif au moyen d'un plugin Outlook.
- L'utilisateur peut ajouter un expéditeur en liste blanche
- L'utilisateur peut ajouter un expéditeur en liste d'avertissement (si un message en provenance d'un expéditeur de la liste est bloqué, un message d'avertissement est transmis sur l'email de l'utilisateur)

En complément de ce filtrage externe, un antivirus installé sur le serveur de messagerie (McAfee TotalVirus Defense) permet de filtrer de façon centralisée d'éventuels virus résiduels.

Bien qu'il soit encore trop tôt pour tirer le bilan de cette nouvelle protection anti-spam, les premiers résultats sont positifs. La mise à disposition d'options permettant une gestion personnalisée des spams n'a pas posé de problèmes.

Conclusion

Né avec l'apparition des premiers réseaux, le spam a rapidement tiré parti des possibilités offertes : toucher un grand nombre de destinataires, aisément et à un coût raisonnable. Initialement connu comme étant une simple utilisation détournée occasionnelle, le spam a évolué au fil du temps jusqu'au point de générer une véritable économie souterraine. Cette progression fulgurante est principalement causée par les rapides progrès technologiques en la matière : réservé à l'époque à un cercle d'utilisateurs restreints et privilégiés, le réseau mondial actuel est plus vaste, plus performant et de moins en moins coûteux. Rétrospectivement, une telle expansion du spam n'est donc pas réellement surprenante.

Les enjeux d'un tel outil de communication auraient pourtant pu nous laisser penser à l'époque que les dérives du spam ne pourraient pas durer bien longtemps. Aujourd'hui, le constat est très différent : ces années passées pendant lesquelles des mesures ont été prises tant sur le plan technique que juridique ont clairement montré que nous sommes toujours désarmés face au spam.

Comme nous l'avons constaté lors de ce travail, cela provient notamment du fait que la plupart des efforts sont concentrés dans la conception de systèmes défensifs qui permettent de bénéficier d'une protection généralement satisfaisante, mais qui ne traitent pas le problème à la base. D'autre part, certaines techniques conçues pour s'attaquer au spam sont difficilement applicables car elles nécessiteraient une mobilisation au niveau mondial pour être efficaces. Ajoutons également que le spam est très réactif, ce qui lui permet de retrouver rapidement un haut niveau d'efficacité même lorsque la lutte anti-spam frappe un grand coup. Pour illustrer cela, prenons l'exemple de la déconnexion début novembre 2008 de l'entreprise californienne McColo Corp. ayant mis hors service un certain nombre de botnets. Alors que la chute du nombre de spam fut spectaculaire (chiffrée entre -66 à -75%), le volume est rapidement remonté au niveau habituel de ces derniers temps [ZNET02] [SPC].

Le meilleur moyen d'anéantir le spam serait de ne pas y participer. Malheureusement, l'ampleur du problème montre qu'il s'agit toujours d'un marché très lucratif (notamment par la diversification des attaques), malgré la certaine prise de conscience des internautes ces dernières années.

Si vaincre le spam est pour l'instant un objectif inatteignable, prendre des mesures pour s'en prémunir reste la seule possibilité. Comme nous l'avons vu, le choix d'une

solution anti-spam est fortement lié au contexte de l'entreprise. Il n'existe donc pas de solution anti-spam universelle, chaque entité doit faire un choix adapté à sa situation.

De façon générale, la réalisation de ce travail a été très enrichissante car elle a permis de faire le point sur les transformations successives liées au spam. La principale difficulté rencontrée lorsqu'on s'intéresse à ces événements passés est que l'information est très peu structurée. Internet regorge d'articles à ce sujet, mais une fois publiés, ils se retrouvent rapidement noyés dans le flot des nouvelles quotidiennes. Relever les éléments essentiels d'un certain aspect du spam tout en respectant la chronologie peut être un exercice long et délicat. Cet état de l'art permet donc de combler ce manque d'informations consolidées.

La suite du travail traitant des solutions anti-spam a quant à elle été intéressante par son côté pratique.

Bibliographie

Sites web & articles

[01N01] Rédaction 01net. L'inventeur du Spam à nouveau débouté. In : *Site d'information 01net* [en ligne]. http://www.01net.com/article/328775.html (consulté le 24.09.08)

[01N02] Rédaction 01net. Les critères de choix pour les logiciels de filtrage. In : *Site d'information 01net* [en ligne]. http://www.01net.com/article/150921.html (consulté le 23.10.08)

[01N03] Rédaction 01net. Zones d'ombre autour des listes noires antispam. In : *Site d'information 01net* [en ligne]. http://www.01net.com/editorial/257353/zones-d-ombre-autour-des-listes-noires-antispam/ (consulté le 02.11.08)

[01N04] Rédaction 01net. Vérifiez si vos e-mails sont considérés comme du spam. In : *Site d'information 01net* [en ligne]. http://www.01net.com/editorial/350120/verifiez-si-vos-e-mails-sont-consideres-comme-du-spam/ (consulté le 14.11.08)

[AFR] Atelier.fr. Comment mettre en place un projet anti-spam au sein d'une grande entreprise ?. In : *Site d'information « Atelier.fr » (BNP Paribas)* [en ligne]. http://www.atelier.fr/article.php?artid=26910&type=CRConference (consulté le 27.11.08)

[AKI] Akismet. Stats Page (beta). In : *Site de l'éditeur Akismet (solution anti-spam pour bloggeurs)* [en ligne]. http://akismet.com/stats/ (consulté le 13.10.08)

[AMAC] AméliorAction. Ce qu'un décideur veut savoir avant d'investir sur l'Internet (suite). In : *Site de conseil AméliorAction (Conseil et formation stratégie d'entreprise et gestion IT)* [en ligne]. http://www.amelioraction.ca/batisseurs/decid-2.htm (consulté le 24.09.08)

[AOS] Oktey. Panorama des technologies antispam. In : *Site de l'ISP ALTOSPAM* [en ligne]. http://www.altospam.com/fr/panorama-des-technologies-antispam.php (consulté le 01.11.08)

[ARO] Arobase. Le spam a 30 ans ! . In : *Site Arobase.org, ressource francophone sur le courrier électronique* [en ligne]. http://www.arobase.org/culture/premier-spam.htm (consulté le 24.09.08)

[ARPA] Wikipédia. ARPANET. In : *Encyclopédie libre Wikipédia* [en ligne]. http://fr.wikipedia.org/wiki/Arpanet (consulté le 24.09.08)

[BAN] Barracuda Networks. Annual Spam Report. In : *Site de l'éditeur Barracuda Networks* [en ligne]. http://www.barracudanetworks.com/ns/news_and_events/index.php?nid=232 (consulté le 17.10.08)

[BITD] BitDefender. *Archive des actualités BitDefender* [en ligne]. http://www.bitdefender.fr/site/News/newsArchive/ (consulté le 02.10.08)

[CNIL01] CNIL. SPAM : définitions. In : *Site de la CNIL* [en ligne]. Modifié le 02.03.05. http://www.cnil.fr/index.php?id=1533 (consulté le 22.09.08)

[CNIL02] CNIL. Analyse de la "boîte à spam". In : *Site de la CNIL* [en ligne]. Modifié le 22.07.04. http://www.cnil.fr/index.php?id=1271 (consulté le 11.10.08)

[CNIL03] CNIL. SPAM : L'état du droit en Europe. In : *Site de la CNIL* [en ligne]. Modifié le 23.07.04. http://www.cnil.fr/index.php?id=1634 (consulté le 19.10.08)

[CNIL04] CNIL. SPAM : L'état du droit en France. In : *Site de la CNIL* [en ligne]. Modifié le 05.09.06. http://www.cnil.fr/index.php?id=1272 (consulté le 19.10.08)

[CNN] NICCOLAI, James. China seen as a growing source of spam. In : *Site d'information CNN* [en ligne]. http://transcripts.cnn.com/2000/TECH/computing/04/06/chinese.spam.idg/index.html (consulté le 25.09.08)

[COM] Commtouch. 2006 Spam Trends Report. In : *Site de l'éditeur Commtouch* [en ligne]. http://www.commtouch.com/documents/commtouch_2006_spam_trends_year_of_the_zombies.pdf (consulté le 15.10.08)

[CORT] Cortina. Passerelle Sécurisée de Messagerie. *Site de l'entreprise en conseil IT « Cortina »* [en ligne]. http://www.cortina.fr/_ironport-passerelle-securisee-messagerie.php (consulté le 15.11.08)

[DDM] Direction du développement des médias. In : *Site français de la direction du développement des médias* [en ligne]. Modifié le 21.09.05. http://www.ddm.gouv.fr/article.php3?id_article=600 (consulté le 19.10.08)

[DLM] Demain le mail. La diffusion de spam bientôt légalisée aux USA ? In : *Blog Demain le mail* [en ligne]. http://www.demainlemail.com/?p=124 (consulté le 19.10.08)

[DRM] DirectoryM. Making Your Anti-spam Solution Work. In : Site d'information *« DirectoryM.net »* [en ligne]. http://articles.directorym.net/Making_Your_Anti_spam_Solution_Work-a946550.html (consulté le 27.11.08)

[EXP] L'expansion.com. 100.000 blogs créés par jour, mais combien de "splogs" ? In : *Site d'information L'Expansion.com* [en ligne].

http://www.lexpansion.com/economie/actualite-high-tech/100-000-blogs-crees-par-jour-mais-combien-de-splogs_117403.html (consulté le 13.10.08)

[FR24] DE SCITIVAUX, Nicolas. L'explosion de l'Internet en Chine. In : *Site de la chaîne de télévision française France 24* [en ligne]. http://www.france24.com/fr/20080801-Chine-explosion-internet-millions-Etats-Unis (consulté le 26.09.08)

[GART] Gartner. Gartner Survey Shows Phishing Attacks Escalated in 2007. In : *Site de l'institut Gartner* [en ligne]. http://www.gartner.com/it/page.jsp?id=565125 (consulté le 08.10.08)

[GASP] Guide ANTI-SPAM. Services de filtrage externalisé. In : *Site d'information sur le spam « Guide ANTISPAM »* [en ligne]. http://www.anti-spam.fr/services_de_filtrage_externalise.html (consulté le 01.11.08)

[GFI01] GFI. Comment garder le spam à l'écart de votre réseau. In : *Site de l'éditeur GFI* [en ligne]. http://www.gfi.com/fr/whitepapers/block-spam-from-your-network.pdf (consulté le 31.10.08)

[GFI02] GFI. Software vs. Appliances. In : *Site de l'éditeur GFI* [en ligne]. http://www.gfi.com/pages/softwarevs.htm (consulté le 31.10.08)

[GFI03] GFI. GFI MailEssentials 14 - Manual. In : *Site de l'éditeur GFI* [en ligne]. http://www.gfi.com/mes/me14manual.pdf (consulté le 09.11.08)

[GNT01] Génération-NT. Les mobiles sont-ils la prochaine forme des botnets ? In : *Site d'information Génération-NT* [en ligne]. http://www.generation-nt.com/mobiles-hyptothese-botnet-spam-georgia-tech-actualite-170611.html (consulté le 16.10.08)

[GNT02] Génération-NT. Les botnets se multiplient mais leur taille diminue. In : *Site d'information Génération-NT* [en ligne]. http://www.generation-nt.com/botnets-reseaux-machines-esclaves-actualite-45655.html (consulté le 16.10.08)

[GNT03] Génération-NT. SymbOS/Kiazha.A : du racket mobile chinois pour Symbian OS. In : *Site d'information Génération-NT* [en ligne]. http://www.generation-nt.com/symbos-kiazha-malware-mobile-chine-mcafee-actualite-69329.html (consulté le 18.10.08)

[GNT04] Génération-NT. Le spam devient psychologue. In : *Site d'information Génération-NT* [en ligne]. http://www.generation-nt.com/commenter/mcafee-spam-experience-actualite-116011.html (consulté le 22.10.08)

[GREY] Wikipédia. Greylisting. In : *Encyclopédie libre Wikipédia* [en ligne]. http://fr.wikipedia.org/wiki/Greylisting (consulté le 02.11.08)

[GSMO1] Global Security Mag Online. G DATA : Les faux anti-spyware innondent le web ! In : *Site d'information Global Security Mag* [en ligne]. http://www.globalsecuritymag.fr/G-DATA-Les-faux-anti-spyware,20081003,5303 (consulté le 16.10.08)

[GSMO2] Global Security Mag Online. Sophos protège contre les pourriels avec "Sender Genotype". In : *Site d'information Global Security Mag* [en ligne]. http://www.globalsecuritymag.fr/Sophos-protege-contre-les,20080728,4218 (consulté le 18.11.08)

[HAS02] AOUN, Frédéric, RASLE, Bruno. Faut-il craindre les effets pervers des parades anti-spam ? In : *Site du livre « Halte Au Spam »* [en ligne]. http://www.halte-au-spam.com/Effets-pervers.pdf (consulté le 03.11.08)

[HASH] Wikipédia. Fonction de hachage. In : *Encyclopédie libre Wikipédia* [en ligne]. http://fr.wikipedia.org/wiki/Fonction_de_hachage (consulté le 03.11.08)

[HSC] Hervé Schauer. Lutter contre le spam. In : *Site du cabinet de consulting « Hervé Schauer »* [en ligne]. http://www.hsc.fr/ressources/presentations/netsec04-spam/netsec04-spam.pdf (consulté le 23.11.08)

[IDXL01] THEVENON, David. Externaliser 15 passerelles anti-spam et anti-virus. In : *Indexel.net, le site des décideurs informatiques* [en ligne]. http://www.indexel.net/1_6_3830__3_/2/12/1/15_passerelles_anti-spam_et_anti-virus.htm (consulté le 23.10.08)

[IDXL02] SAIZ, Jérôme. Externaliser la sécurité de sa messagerie : la clé de la tranquillité. In : *Indexel.net, le site des décideurs informatiques* [en ligne]. http://www.indexel.net/1_6_4119__3_/2/12/1/Externaliser_la_securite_de_sa_messagerie___la_cle_de_la_tranquillite.htm (consulté le 01.11.08)

[IKS] IKS. Teergrubing FAQ. In : *Site de l'entreprise IKS* [en ligne]. http://www.iks-jena.de/mitarb/lutz/usenet/teergrube.en.html (consulté le 03.11.08)

[INS] NIEL, Xavier ; JLASSI Mahmoud. Premiers résultats de l'enquête TIC 2007 auprès des entreprises. In : *Site de la Direction du Commerce, de l'Artisanat, des Services et des Professions libérales* [en ligne]. http://www.pme.gouv.fr/economie/commissions/122007-TIC.pdf (consulté le 29.10.2008)

[IRON] IronPort. 2008 Internet Security Trends : Emerging Attack Platforms for Spam, Viruses and Malware. In : *Site de la société IronPort* [en ligne]. http://pages.ironport.com/trendsreport2008.html?source=trends_2008 (consulté le 29.09.08)

[ITPR01] iTPro. Comment traiter le SPAM ? In : Portail des technologies informatiques d'entreprise « iTPro » [en ligne]. http://exchange.itpro.fr/Dossiers-par-Theme/suivante/2/12/200892687-Comment-traiter-le-SPAM-.htm (consulté le 31.10.08)

[ITPR02] iTPro. Sophos ES4000 Security Appliance. In : Portail des technologies informatiques d'entreprise « iTPro » [en ligne]. http://www.itpro.co.uk/150666/sophos-es4000-security-appliance (consulté le 20.11.08)

[ITU] International Telecommunication Union (ITU). Internet user penetration rates worldwide and for developed and developing regions, between 1997 and 2007. In : *Site de l'ITU* [en ligne]. http://www.itu.int/ITU-D/ict/statistics/ict/graphs/internet.jpg (consulté le 30.10.2008)

[IWOR] InfoWorld. Lab test: Cisco IronPort. In : *Site d'information « InfoWorld »* [en ligne]. http://www.infoworld.com/article/08/04/09/15TC-mail-security-cisco_1.html (consulté le 15.11.08)

[JDN01] JDN. Fraude 419 : le spam qui venait d'Afrique. In : *Site du Journal Du Net* [en ligne]. http://www.journaldunet.com/0306/030623fraude419.shtml (consulté le 09.10.08)

[JDN02] JDN. Le spam plus que jamais polyglotte. In : *Site du Journal Du Net* [en ligne]. http://www.journaldunet.com/solutions/securite/actualite/le-spam-plus-que-jamais-polyglotte.shtml (consulté le 11.10.08)

[JDN03] JDN. Spams SMS : comment Orange tente de faire face. In : *Site du Journal Du Net* [en ligne]. http://www.journaldunet.com/0209/020923orange.shtml (consulté le 12.10.08)

[JDN04] JDN. Spams SMS : Armer ses passerelles et serveurs de messageries contre le spam. In : *Site du Journal Du Net* [en ligne]. http://www.journaldunet.com/solutions/0607/060719-panorama-anti-spam/1.shtml (consulté le 23.10.08)

[JDN05] JDN. Comment Arte France sous-traite sa gestion des spams. In : *Site du Journal Du Net* [en ligne]. http://www.journaldunet.com/0209/020923orange.shtml (consulté le 01.11.08)

[JDN06] JDN. Spam, la marée noire perdure. In : *Site du Journal Du Net* [en ligne]. http://www.journaldunet.com/solutions/0701/070115-spam-lutte-greylisting.shtml (consulté le 02.11.08)

[JDN07] JDN. Les disques durs encore peu fiables. In : *Site du Journal Du Net* [en ligne]. http://www.journaldunet.com/solutions/0702/070222-disque-dur-google.shtml (consulté le 17.11.08)

[KANO] Kanopea. Un générateur d'expressions régulières antispam. In : *Blog d'actualités de la messagerie électronique et du spam « Kanopea »* [en ligne]. http://blog.kanopea.fr/2007/09/14/un-generateur-dexpressions-regulieres-antispam/ (consulté le 01.11.08)

[LASP] Logiciel-antispam. Choisir son logiciel anti spam. In : *Site d'information généraliste sur le spam « logiciel-antispam.com »* [en ligne]. http://www.logiciel-antispam.com/ (consulté le 01.11.08)

[LENO] SAIZ, Jerome. La fin de la solution antispam miracle ? In : Site d'information LesNouvelles.net [en ligne]. http://www.lesnouvelles.net/articles/produits/spam-challenge-response-pire-que-le-mal (consulté le 20.10.08).

[LNX01] Da Linux French Page. Tout ce que vous avez voulu savoir sur le spam sans jamais avoir osé le demander. In : *Site de LinuxFR.org* [en ligne]. http://linuxfr.org/2003/06/23/12931.html (consulté le 24.09.08)

[LNX02] Da Linux French Page. Rions un peu avec les spams traduits. In : *Site de LinuxFR.org* [en ligne]. http://linuxfr.org/~gabygaby/26651.html (consulté le 11.10.08)

[LNX03] Da Linux French Page. Tout ce que vous avez voulu savoir sur le spam sans jamais avoir osé le demander. In : *Site de LinuxFR.org* [en ligne]. http://linuxfr.org/2003/06/23/12931.html (consulté le 24.09.08)

[LTPS] HAEBERLI, David. Le spam est en train de couler Internet. In : *Site du journal Le Temps*. http://www.letemps.ch/dossiers/dossiersarticle.asp?ID=97379 (consulté le 21.10.08)

[MARS] Marshal. Sex, Drugs and Software Lead Spam Purchase Growth. In : *Site de l'éditeur Marshal* [en ligne]. http://www.marshal.com/pages/newsitem.asp?article=748&thesection=news (consulté le 22.10.08)

[MCL] MailCleaner. Que peut-on entreprendre contre le "spamming" sur le plan juridique ? In : Site de l'éditeur MailCleaner [en ligne]. http://www.mailcleaner.net/docs/law_fr.html (consulté le 19.10.2008)

[MEX01] MSExchange. Server Based Antispam Comparison. In : *Site d'information « MSExchange » sur les ressources Exchange* [en ligne].

http://www.msexchange.org/articles/Server_Based_Antispam_Comparison.html (consulté le 10.11.08)

[MEX02] MSExchange. Voted MSExchange.org Readers' Choice Award Winner. In : *Site d'information « MSExchange » sur les ressources Exchange* [en ligne]. http://www.msexchange.org/ExchangeNews/general/MSExchange-Readers-Choice-Award-Exchange-AntiSpam-GFI-MailEssentials-Jun08.html (consulté le 10.11.08)

[MFR] MailFrontier. Putting Anti-Spam Solutions to the Test...Before You Buy. In : *Site de l'éditeur « SonicWALL » (anciennement MailFrontier)* [en ligne]. http://www.mailfrontier.com/docs/how_to_test.pdf (consulté le 26.11.08)

[MIB] MailInBlack. CP / a la recherche de l'antispam ideal. In : *Site de l'éditeur MailInBlack* [en ligne]. http://www.mailinblack.fr/site/upload/21-03-2008_Premier-Cercle.pdf (consulté le 08.11.08)

[MRGZ] MACDONALD, Don. Quebecer fined in pump and dump scheme. In : *Site de Montreal Gazette* [en ligne]. http://www.canada.com/montrealgazette/news/business/story.html?id=fdbbb55c-ac8a-4bdc-bcac-3d30fdaaa754 (consulté le 02.10.08)

[MTK] MessagingTalk. Product Review: GFI Mailessentials. In : *Site d'information « MessagingTalk » sur les ressources Exchange* [en ligne]. http://www.messagingtalk.org/product-review-gfi-mailessentials (consulté le 09.11.08)

[OPUS] Opus One. Results of Anti-Spam Solution Testing. In : *Site de l'entreprise de consulting « Opus One »* [en ligne]. http://www.opus1.com/www/whitepapers/antispamfeb2007.pdf (consulté le 15.11.08)

[OSSIR] PRIGENT, Fabrice. *Retour d'expérience sur le greylisting du courrier électronique*. In : Site de l'OSSIR [en ligne]. http://www.ossir.org/resist/supports/cr/20050627/CR-ReSIST-2005-06-27.pdf (consulté le 02.11.08)

[PCWD] CHAUSSON, Cyrille. Un million d'ordinateurs entre les mains de onze botnets. In : *Site d'information PCWorld* [en ligne]. http://www.pcworld.fr/actualite/million-ordinateurs-entre-mains-onze-botnets/6131/ (consulté le 15.10.08)

[PNEX] FREOR, Jean. Les Filtres Antispam. In : *Site d'information PopNext* [en ligne]. http://popnext.generationmp3.com/files/misc_janvier_2005/Rapport_Jean_Filtres_antispam.pdf (consulté le 23.10.08)

[PSZO] Pro Security Zone. Fake e-mail delivery messages contain Trojan. In : *Site d'information Pro Security Zone* [en ligne]. http://www.prosecurityzone.com/Customisation/News/IT_Security/Anti-virus_and_anti-malware_software/Fake_e-mail_delivery_messages_contain_Trojan.asp (consulté le 16.10.08)

[SAGE] SAGE. Ironport vs. Barracuda cagematch. In : *Site d'information pour sysadmins « SAGE »* [en ligne]. http://www.sage.org/lists/sage-members-archive/2005/msg02991.html (consulté le 15.11.08)

[SAS01] SpamAssassin. Tests Performed: v3.2.x. In : *Site web du projet open-source SpamAssassin* [en ligne]. http://spamassassin.apache.org/tests_3_2_x.html (consulté le 01.11.08)

[SAS02] Wikipédia. SpamAssassin. In : *Encyclopédie libre Wikipédia* [en ligne]. http://fr.wikipedia.org/wiki/Spamassassin (consulté le 21.11.08)

[SBZ] SmallBiz. Les spams interdits en Suisse. In : *Site de la société VisualObject* [en ligne]. http://smallbiz.ch/news.php?newsid=20 (consulté le 19.10.08)

[SCM01] SC Magazine. ScanMail for Microsoft Exchange. In : *Site du magazine « SC Magazine »* [en ligne]. http://www.scmagazineus.com/ScanMail-for-Microsoft-Exchange/Review/529/ (consulté le 13.11.08)

[SCM02] SC Magazine. Winners announced: SC Awards 2008. In : *Site du magazine « SC Magazine »* [en ligne]. http://www.scmagazineus.com/Winners-announced-SC-Awards-2008/article/108722/ (consulté le 15.11.08)

[SECU] GALLOT, Kevin. Les méthodes anti-spam. In : *Site d'information sur la sécurité « Secuser »* [en ligne]. http://www.secuser.com/dossiers/methodes_antispam.htm (consulté le 01.11.08)

[SILI01] DIMBERTON, Arnaud. Google se penche sur le phishing 2.0. In : *Site d'information Silicon.fr* [en ligne]. http://www.silicon.fr/fr/news/2007/12/11/google_se_penche_sur_le_phishing_2_0 (consulté le 08.10.08)

[SILI02] Silicon. Un "Roi du spam" retrouvé mort. In : *Site d'information Silicon.fr* [en ligne]. http://www.silicon.fr/fr/news/2008/07/28/un__roi_du_spam__retrouve_mort (consulté le 19.10.08)

[SOPH01] Sophos. *Archives des actualités Sophos* [en ligne]. http://www.sophos.fr/pressoffice/news/articles/2008/ (consulté le 19.09.08)

[SOPH02] Sophos. *Sophos Email Appliances* [en ligne]. http://www.sophos.com/products/enterprise/email/security-and-control/appliances/specs.html (consulté le 17.11.08)

[SOPH03] Sophos. *Sophos Email Appliances*. In : *Site de l'éditeur Sophos* [en ligne]. http://www.sophos.com/images/products/enterprise/es_applianceProcess.jpg (consulté le 17.11.08)

[SOPH04] eVision IT. Appliances des messagerie pour le marché des PME. *Site de l'éditeur Sophos* [en ligne]. http://fr.sophos.com/sophos/docs/fra/marketing_material/evision-email-appliance-review_dec07-fr.pdf (consulté le 20.11.08)

[SPC] SpamCop. SpamCop Statistics. In : *Site « SpamCop »* [en ligne]. http://www.spamcop.net/spamgraph.shtml?spamyear (consulté le 06.12.08)

[SYM01] CONLEY, Kelly. Where do Bounce Messages come From? In : *Site de l'éditeur Symantec* [en ligne]. https://forums.symantec.com/syment/blog/article?message.uid=332236 (consulté le 16.10.08)

[SYM02] CONLEY, Kelly. Image Spam Trying a Comeback - Without Success. In : *Site de l'éditeur Symantec* [en ligne]. https://forums.symantec.com/syment/blog/article?message.uid=357793 (consulté le 16.10.08)

[SYSC] SYS-CON Media. Lowest Total Cost of Ownership. In : *Site d'information SYS-CON Media* [en ligne]. http://www.sys-con.com/node/495381 (consulté le 13.11.08)

[TDM01] TrendMicro. Manuel TrendMicro ScanMail. In : *Site de l'éditeur TrendMicro* [en ligne]. http://www.trendmicro.com/ftp/documentation/guides/smex-v7-ag.pdf (consulté le 12.11.08)

[TDM02] TrendMicro. ScanMail™ Suite for Lotus™ Domino™. In : *Site de l'éditeur TrendMicro* [en ligne]. http://fr.trendmicro.com/imperia/md/content/fr/products/datasheets/ds06smld3_080310fr.pdf (consulté le 12.11.08)

[TOMS] AGUILA, Nicolas. Une nouvelle forme de phishing se montre. In : *Site d'information Tom's Guide.com / Infos-du-Net.com* [en ligne]. http://www.infos-du-net.com/actualite/6874-phishing.html (consulté le 08.10.08)

[WASH] MCGUIRE, David. One Year After Law, Spam Still Out of the Can. In : *Site du Washington Post* [en ligne]. http://www.washingtonpost.com/wp-dyn/articles/A44124-2005Jan3.html (consulté le 19.10.08)

[WCL] West Coast Labs. GFI Mail Essentials for Exchange/SMTP. In : *Site de « West Coast Labs », spécialiste tests & certifications* [en ligne]. http://www.westcoastlabs.com/downloads/productTestReport_0013/MailEssentials_for_Exchange.pdf (consulté le 10.11.08)

[ZNET01] DUMOUT, Estelle. Microsoft modère ses ambitions avec Sender ID. In : *Site d'information ZDNet* [en ligne]. http://www.zdnet.fr/actualites/internet/0,39020774,39247895,00.htm (consulté le 22.10.08)

[ZNET02] VAMOSI, Robert. Chute brutale des spams envoyés après la fermeture d'un hébergeur. In : *Site d'information ZDNet* [en ligne]. http://www.zdnet.fr/actualites/internet/0,39020774,39384849,00.htm (consulté le 06.12.08)

[ZSP] ZeroSpam. Évaluation comparée des solutions existantes. In : *Site de l'éditeur ZeroSpam* [en ligne]. http://www.zerospam.ca/1/Carnet_spam/Osez_comparer#h3310 (consulté le 31.10.08)

Ouvrages & rapports

[AKS] GALLOT, Kevin. Anti-Spam : Kit de survie. Paris : Editions Dunod, 2004. 208 p. ISBN 2-100-48643-8

[ASTK] WOLFE, Paul ; SCOTT Charlie ; ERWIN, Mike. Anti-Spam Tool Kit. Emeryville, CA, 2004. 400 p. ISBN 0-072-23167-X

[HAS01] AOUN, Frédéric, RASLE, Bruno. Halte au Spam. Paris : Editions Eyrolles, 2003. 312 p. ISBN 2-212-11307-2

[ISN99] HAURI, Rolf. Stratégie anti-spam pour l'entreprise. ISNet 99. Rapport final. Septembre 2006.