



HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

**Groupe de contact sur le spam
16 Janvier 2004**

Éléments de réflexion sur le spam

Hervé Schauer
<Herve.Schauer@hsc.fr>

- x Contexte général
- x Contexte du spam dans la société
- x Solutions techniques de lutte contre le spam
- x Limites de la lutte contre le spam
- x Absence de dialogue et de déontologie
- x Quel futur ?
- x Suggestions
- x Ressources

- x Multiples formes de spam
 - x Les boites aux lettres de courrier postal sont remplies de publicités papier adressés nominativement qui n'ont jamais été sollicitées
 - x Très difficile de retrouver la société à l'origine du délit
 - x celle qui a vendu, celle qui n'a pas respecté le choix de l'utilisateur qui ne souhaitait pas la diffusion de son adresse,
 - x chaque fusion/rachat/etc est l'occasion d'échanges de fichiers en remettant tout à zéro
 - x les sociétés mentent systématiquement
 - x Loi informatique et libertés virtuelle
 - x pas de condamnations significatives
 - x pas ou peu de condamnations spécifiques à cette loi
 - x pas le rôle ni les moyens pour les victimes particuliers ou professionnels de porter plainte
 - x pas d'organisme qui se saisit pour pallier à l'absence de plainte des victimes
 - x état, entreprises publiques et collectivités ne montrent pas l'exemple et leurs fichiers ont été utilisés pour des envois de publicités nominatives non-sollicitées

- x Multiples formes de spam (*suite*)
 - x Les lignes téléphoniques privées et professionnelles reçoivent perpétuellement des appels non-sollicités
 - x Pour des cuisines même lorsque l'on a jamais acheté de cuisine de sa vie
 - x Même lorsque l'on est sur la liste orange
 - x Il est généralement difficile de connaître le nom de la société de marketing téléphonique
 - x Il est généralement difficile de retrouver le commanditaire original
- x Ces problèmes de spam dont le public est victime ne sont pas gérés par la société → la gestion du spam par courrier électronique ne va pas être une tâche facile

- x Le spam de courriel a un coût proche de zéro, il est la plus rentable de toutes les formes de spam pour le spammeur, il ne risque pas de s'évaporer
- x Le spam pourra toujours être émis par un particulier ou une entreprise dans un paradis juridique
- x → Toute mesure hexagonale de contrôle très contraignante aura une portée limitée et déportera la source du problème ailleurs, avec probablement des possibilités d'enquête et juridiques moindres
- x Les rares cas de délinquance informatique organisée sont majoritairement liés au spam et à son intérêt, cf. Sobig cet été
- x → Un contrôle législatif trop poussé du spam peut risquer de le faire migrer vers les activités maffieuses

- x Les spammeurs français ne sont pas inquiétés
 - x Ils contreviennent pourtant tous à la législation existante
- x Il est souhaitable d'agir et d'obtenir des résultats chez soi, pour s'ouvrir la possibilité ensuite d'agir à l'international
- x A l'échelle hexagonale, il faut d'abord commencer par se donner les moyens d'appliquer la législation existante
- x Cela pourrait avoir pour conséquence le développement d'une auto-régulation en France de la part de la profession du marketing en ligne

- x Le spam de courriel a l'avantage d'autoriser des solutions techniques là où les autres formes de spam n'en ont pas d'aussi accessibles
 - x Possibilité d'analyse sémantique pour éliminer un grand nombre de spam
 - x Plusieurs logiciels sur le marché dont le logiciel libre spamassassin
 - x Possibilité d'utiliser des adresses à usage unique, permettant de tracer l'usage illégal ou abusif d'une adresse fournie à un tiers dans un cadre donné
 - x Les informaticiens utilisent un domaine personnel et des adresses dans leur domaine pour chaque usage
 - x Ce type de service est par exemple proposé en infogérance pour les opérateurs par Dolphian en France
 - x AOL par exemple intègre la lutte anti-spam en standard
 - x Mais ils interdisent les utilisateurs ayant des adresses dynamiques ce qui apporte plus de problèmes que cela résoud de solutions
 - x Possibilité d'utiliser des adresses pot de miel pour repérer les spammeurs
 - x Pour une adresse électronique publiée, associer aussi une adresse pot de miel
 - x Obliger une modification manuelle de l'adresse

- x La gestion du spam pour une victime est actuellement réaliste
 - x 200 spams par jour, capturés à 90% par spamassassin sans faux-positif, coutent environ 5 à 10 minutes
 - x pas plus que de traiter le courrier postal quotidien qui est de la publicité non-sollicitée
 - x pas plus que 2 appels téléphoniques non-sollicités
 - x pas plus que de traiter une candidature pour un emploi qui n'est pas proposé par la société
- x Mais la gestion du spam devient irréaliste
 - x Le nombre de spams reçus chaque jour est en constante augmentation
 - x Le taux de réussite des logiciels anti-spam est en baisse, légère, mais régulière, malgré leurs propres progrès
 - x La mise à jour du logiciel anti-spam doit être régulière
 - x Pas aussi simple qu'une base de signatures d'anti-virus

- x La gestion du spam devient irréaliste (*suite*)
 - x Le spam est de plus en plus difficile à trier
 - x Le spam est de plus en plus difficile à filtrer
 - x Le développement de l'abus de fonctionnalités inutiles (HTML) augmente les faux-positifs
 - x Le CPU nécessaire à la détection du spam devient important
 - x Ce n'est plus dans les possibilités de la majorité des fournisseurs d'accès
 - x L'organisation de la lutte contre le spam est un projet, un métier, à part entière dans les entreprises, et un coût de plus en plus important
 - x Comment avoir un système permettant à chaque personne de manière simple de signaler un spam qui n'a pas été reconnu ?
 - x Microsoft Outlook et Lotus Notes reformattent de manière irréversible le message d'origine et ses en-têtes, interdisant la lutte anti-spam
 - x Les spammers contournent de mieux en mieux les dispositifs techniques de lutte contre le spam

- x Lors d'une enquête, les sociétés de spam mentent
 - x Elles le font déjà dans le cas des spams par courrier postal
 - x Elles mentent systématiquement pour le spam de courrier électronique
 - x Par téléphone, en général elles ne répondent pas au courrier électronique
- x Le vécu avec les sociétés de spam
 - x Utilisation de bases récupérées sur des serveurs victimes de piratages
 - x Envoi de spam sans domaine source, sans aucune possibilité de tracer l'origine
 - x Envoi de spam à partir de comptes créés automatiquement sur les courrielwebs
 - x Utilisation de toutes les techniques pour avoir la tracabilité de la cible : HTML, *webbugs*, *cookies*, etc

- x Un modèle fermé à base du principal produit propriétaire du marché
 - x Payant
 - x Garanti sans spam
 - x Comme le code mobile signé peut être garanti sans code malveillant ?
- x Un modèle où le courriel est facturé à l'émetteur
 - x Certification du serveur de l'entreprise pour envoyer du courriel
 - x Authentification des serveurs, certificats & filtrage IP
 - x Acceptation des messages que de ceux qui ont payé l'envoi
 - x Paiement au message envoyé pour les particuliers
- x ➔ A qui celà profitera ?
- x Un développement de l'usage de la signature des messages
 - x PGP, X.509

- x Faire appliquer la loi informatique et libertés par un tiers au frais de la collectivité
- x Faire un sorte que la profession impose qu'un message publicitaire comporte la preuve irréfutable qu'il a été sollicité et qu'il n'est pas un spam
 - x Indiquer ou et quand l'adresse du destinataire a été fournie et par qui
 - x Rappeller que l'autorisation a été donnée à cette occasion de faire usage de son adresse pour recevoir des informations
 - x Lui indiquer quel est le fichier qui contient son adresse, avec son propriétaire identifié par son siret

Questions ?

www.hsc.fr

Herve.Schauer@hsc.fr

- x Spamassassin, <http://www.spamassassin.org/>
- x Présentation de spamassassin, Denis Ducamp, HSC, OSSIR SUR, 11/02,
<http://www.hsc.fr/ressources/presentations/spamassassin/>
- x Synthèse de l'atelier sur le spam, Hervé Schauer, HSC, ISOC/Journées d'Autrans, 01/98,
<http://www.isocfrance.org/archives/AUTRANS98/at-abus.htm>
- x Pour me connaître :
 - x Biographies : http://www.hsc.fr/societe/herve_schauer.html.fr
http://www.solutionslinux.fr/fr/conferencier_detail.php?id_conferencier=68
 - x HSC : <http://www.hsc.fr/societe/>
 - x Associations : AFUL, AFUP, CLUSIF, IEEE, FNTC, IALTA, IETF, ISACA, ISOC, ISSA, CES, OSSIR, SAGE, SANS, SEE, USENIX,
<http://www.hsc.fr/societe/associations.html>