



Éditorial

# L'invasion des SPAM images

Guillaume Lehembre 

**V**ous êtes très certainement confrontés depuis plusieurs mois à une recrudescence des SPAM dans vos boîtes aux lettres et en particulier des SPAM images. Ces pourriels, comme on les appelle en français, représentent selon diverses études datées de fin 2006 entre 90 et 95% des courriers électroniques circulant sur Internet.

Les adresses emails valides ne sont plus récupérées en les glanant sur Internet ou en les volant dans les carnets d'adresses sur des machines compromises mais elles sont découvertes en faisant des attaques brute-force (plus ou moins intelligentes) sur les comptes SMTP des grands fournisseurs d'accès ou de Webmail. Pas étonnant que votre adresse mail fraîchement créée soit déjà envahie de SPAM peu de temps après, alors que vous n'aviez donné l'adresse à personne !

Le principe des SPAM images est simple, il consiste à envoyer un mail ordinaire avec un corps de message comportant un texte anodin (extrait de livre, chanson, etc.) et une image de faible taille en fichier joint. Le corps du mail est donc fait uniquement pour induire en erreur les filtres anti-SPAM et corrompre leurs filtres bayésiens si un apprentissage est fait sur ces textes, on parle alors de Bayesian Poisoning. Le «message» réel du SPAM est contenu dans l'image et dans un grand nombre de clients mails ou de Webmails populaires, ces images sont affichées au côté du message texte sans qu'aucune action de l'utilisateur ne soit nécessaire.

Les filtres anti-SPAM du marché doivent donc s'adapter à cette nouvelle donne qui représente dorénavant plus de 25% des SPAM envoyés. La méthode la plus simpliste et la plus rapide pour détecter des SPAM images simples est de calculer une empreinte cryptographique sur chaque image reçue en écartant les messages dont l'empreinte fait partie d'une liste de SPAM images connus. Le gros inconvénient de cette solution est que la moindre modification de l'image entraîne une nouvelle empreinte, les spammeurs n'ont donc pas tardé à implémenter des modifications aléatoires de quelques pixels sur les images qu'ils envoyaient. Il devient donc nécessaire d'analyser le contenu de l'image pour pouvoir classifier le message. La méthode la plus courante est d'utiliser

une solution de reconnaissance de caractères de type OCR afin d'extraire le texte contenu dans l'image pour le traiter par la suite avec des règles classiques d'anti-SPAM. Cette reconnaissance s'avère néanmoins coûteuse en ressources pour l'analyse et contournable avec des méthodes de masquage de texte de type *captcha* [1] comme l'ont rapidement compris les spammeurs. En effet, un faible contraste entre le(s) fond(s) de l'image et le texte combiné à des déformations des lettres du message rendent l'extraction du texte sujette à l'erreur, ce qui peut tromper le moteur anti-SPAM pour la détection d'un SPAM. D'autres méthodes plus probabilistes existent, elles sont basées sur l'analyse statistique des données, d'une image et leur positionnement par rapport à des messages considérés comme non désirés ou légitimes.

Des Webmails grand public comme Gmail utilisent des techniques qui leur sont propres s'avérant être très efficaces grâce au très grand nombre de messages qu'ils reçoivent et grâce à l'analyse temporelle qu'ils peuvent faire sur les vagues d'envoi de SPAM.

Le SPAM n'est donc pas prêt de s'éteindre malgré les propos rassurant de certains dirigeants qui prévoient le contrôle des SPAM pour la fin 2006. On ne sait pas quelles nouveautés nous préparent les spammeurs pour contourner les dernières fonctionnalités de nos filtres. Après tout, c'est l'éternel jeu du chat et de la souris en sécurité, on finit par s'habituer à ce que toute protection soit tôt ou tard contournée :-)

[1] <http://fr.wikipedia.org/wiki/Captcha> (wikipédia - projet d'encyclopédie librement distribuable)

## À propos de l'auteur

Guillaume Lehembre est un consultant sécurité français travaillant pour le cabinet HSC depuis 2004. Il a travaillé sur différents audits, études et tests d'intrusion et a acquis une expérience certaine dans la sécurité des réseaux sans fils. Il a réalisé des interventions publiques à ce sujet et a publié plusieurs articles, dont un article dans le numéro 14 de Hakin9 intitulé Sécurité Wi-Fi - WEP, WPA et WPA2. Guillaume tient à remercier Louis Nyffenegger pour ses conseils avisés lors de la rédaction de cet édito. Il peut être contacté à l'adresse suivante : [Guillaume.Lehembre@hsc.fr](mailto:Guillaume.Lehembre@hsc.fr).