



Focus

Panorama des technologies antispam

Stéphane Manhes



Degré de difficulté



Les spams représentent aujourd'hui plus de 50% du trafic email mondial, certaines entreprises françaises comptent plus de 90% de spams parmi leurs emails. Définir une action contre le spam est devenu en quelques années une obligation du DSI.

Avant de parler des technologies anti-spam, il peut être intéressant d'énumérer les différents éléments disponibles lors de la réception d'un email. Pour envoyer un email, un serveur de messagerie, vu sous une IP publique, utilise le protocole SMTP sous le port TCP/25. Lors de la réception d'un email nous sommes donc en mesure de travailler sur les éléments suivants :

- IP émetteur adresse IP publique du serveur émetteur. Cette IP nous permet d'identifier notamment le pays émetteur, ainsi que le propriétaire de l'IP (souvent le FAI).
- Configuration du serveur émetteur : la configuration même du système d'exploitation a une incidence directe sur la manière de communiquer. Le champ HELO, par exemple, utilisé par le serveur de messagerie lors de l'initialisation de la communication dans le protocole SMTP correspond généralement au nom complet du serveur (FQDN) : `/etc/hosts`
- Protocole SMTP : la présence ou non d'une commande, le respect de l'acquittement entre les commandes du protocole et la syntaxe utilisée sont autant d'éléments

permettant de s'assurer de la qualité du serveur émetteur.

- En-tête du mail : il s'agit des champs d'information présents au début d'un message électronique. Le sujet du message correspond par exemple à l'extraction par le client de messagerie du champ d'en-tête `Subject:`. Au sens de la détection antispam, les champs les plus intéressants sont : `Received`, `Subject`, `Message-Id` et `Date`. Pour rappel, le champ `Received` assure la traçabilité d'un email : chaque serveur par lequel un mail transite ajoute un champ `Received`,

Cet article explique...

Dans cet article nous allons décrire les différentes technologies antispam disponibles. Certaines de ces technologies sont extrêmement simples à mettre en place sur un serveur de messagerie, d'autres sont un peu plus complexes à implémenter.

Ce qu'il faut savoir...

Quelques rudiments dans le fonctionnement des DNS et des serveurs de messagerie sont nécessaires à une bonne compréhension du sujet.

en indiquant au minimum l'identifiant interne du message, le serveur d'origine du mail et la date de traitement.

- Corps du mail : Le contenu (on parle du *corps*) à proprement parler du message, le texte, le format ou l'encodage utilisé.
- Pièces jointes et intégration des pièces-jointes (paramètres Mime) : L'encapsulation des pièces jointes, l'encodage utilisé, leur extension et les pièces jointes elles-même peuvent servir lors de l'analyse du message.
- Adresse email et nom de domaine émetteur, configuration du domaine émetteur : Généralement l'adresse email émettrice n'a que très peu d'intérêt dans la détection d'un spam, par contre, le domaine émetteur permet lui de pouvoir effectuer quelques vérifications ou de pouvoir véhiculer via le DNS quelques informations utiles.

À partir de ces divers éléments d'identification d'un message, des technologies se basant pour la plupart sur des informations différentes ont été développées. Bien que le but général de ces technologies soit d'identifier de manière la plus correcte possible si le message reçu est un spam, certaines de ces technologies apportent de la crédibilité à l'émetteur mais ne permettent pas pour autant de qualifier le message.

D'autre part, chacune de ces technologies ne donne pas les mêmes résultats en termes de détection et d'erreur d'analyse. Par exemple, le simple fait de recevoir un email provenant d'un serveur blacklisté ne signifie pas forcément que le mail est un spam. En effet des études ont montré que plus de 85% des sociétés françaises ont été blacklistées !

Enregistrement DNS inversé

Un nom de serveur *mx.toto.com* est toujours associé à une IP. Inversement, une adresse IP peut être associée à un nom de serveur, on parle alors de *reverse dns*. Une méthode simple pour retrouver le

reverse DNS d'une IP est d'effectuer un `ping -a <IP>`. Concrètement, il s'agit d'une requête DNS de type PTR sur l'adresse IP inversée analysée, dans la zone `.in-addr.arpa`.

Plusieurs niveaux d'analyses peuvent être effectués grâce à cela :

- La simple présence d'un reverse DNS peut être un élément de contrainte. Les serveurs de messagerie de AOL, rejettent catégoriquement tout email provenant d'une adresse IP sans reverse DNS. Cela a pour conséquence de générer un grand nombre de faux-positifs mais permet de faire prendre conscience aux Postmasters de l'importance de ce type de configuration.
- Une analyse plus minutieuse consiste à vérifier la corrélation entre l'adresse IP du serveur source et son nom (on vérifie la bijectivité entre l'adresse IP publique d'un serveur et son nom FQDN).
- Plus finement, la correspondance entre le nom FQDN du serveur de mail (passé en argument du champ HELO lors de la communication SMTP) et le nom FQDN du reverse DNS de l'IP émettrice assure de manière quasi certaine de la *qualité* du serveur. Inversement le fait que ces données ne soient pas identiques n'implique rien, car cela n'est pas toujours réalisable (les serveurs de mail en *load-balancing* possèdent chacun des noms différents sous une IP publique identique).

Indépendamment de la valeur technique de cette information, la présence d'un enregistrement DNS inversé, permet d'affecter facilement une IP à un propriétaire par l'intermédiaire du nom de domaine. Cela a pour conséquence théorique de faciliter la corrélation entre un émetteur et une entité juridique.

Validation émetteur

De l'identité théorique de l'émetteur d'un message, nous ne connaissons

que son adresse email. Cependant cette information n'est pas sûre : le protocole SMTP est ouvert, l'adresse email de l'expéditeur peut être usurpée. L'analyse de cette information est donc très souvent sans grand intérêt, d'autant plus que les spammeurs usurpent l'identité d'utilisateurs légitimes et changent systématiquement d'identité.

Adresse email de l'émetteur

L'adresse email de l'émetteur est présente à deux endroits dans un email :

- Au niveau de l'enveloppe SMTP, la commande `MAIL FROM` : identifie l'émetteur d'un message.
- Dans les en-têtes du message, le champ `FROM` : identifie également l'émetteur du message (c'est cette dernière adresse qui est affichée dans les clients de messagerie).

Il arrive que ces deux informations diffèrent sur un message légitime, mais leur comparaison peut servir d'indicatif. L'une est définie par l'expéditeur du message, l'autre par le serveur émetteur à partir du compte utilisateur émetteur, cette dernière est souvent plus juste.

La vérification de *l'existence* d'une adresse email est techniquement possible. Cependant, dans le cas d'un spam, il s'agit rarement de la véritable adresse du spammeur. D'autre part, certaines listes de diffusion utilisent des adresses non attribuées afin d'éviter d'être submergées par des réponses. La vérification de l'existence de l'émetteur refuserait dans ce cas la lettre d'information, il n'est donc pas judicieux d'effectuer ce contrôle.

Domaine de l'émetteur

Contrairement à l'utilisateur de l'adresse émettrice, l'extraction et l'analyse du domaine émetteur peut apporter des informations utiles. Il est par exemple très intéressant de se servir de ce domaine pour vérifier la présence de champs MX dans la zone DNS en question. Cela permet de valider que l'entité émettrice est



bien en mesure de recevoir des emails. Ce simple contrôle ne génère aucun faux-positif et permet de déceler l'utilisation de faux domaines.

Analyse du protocole SMTP

Le protocole SMTP est régi par des RFC (*Requests for Comments*) définies par l'IETF (*Internet Engineering Task Force*). À l'origine du protocole, la RFC 821 date d'août 1982. Elle a été étendue par la RFC 1869 de novembre 1995 pour l'Extended SMTP. La RFC 2821 d'avril 2001 apporte également quelques améliorations. Le principe fondamental : `HELO, MAIL FROM, RCPT TO, DATA` reste évidemment inchangé depuis 1982 pour assurer la compatibilité.

La plupart des règles définies dans ces RFC sont respectées par l'ensemble des éditeurs de serveur de messagerie (attention il existe quelques exceptions, notamment sur le respect des paramètres de la commande `HELO`). Inversement, un grand nombre de spammeurs omettent souvent de les respecter.

Par exemple, le nom du serveur qui envoie le courriel doit être entièrement nommé (FQDN), règle que les spammeurs ne suivent pas toujours. Les postes utilisateurs infectés de virus qui envoient des emails ne sont pas pleinement qualifiés (FQDN), ils émettent le plus souvent des emails sans respecter cette règle.

Analyse heuristique

L'analyse heuristique constitue un ensemble de règles, tirées d'analogies, représentées sous forme d'expressions régulières (`regexp`). Le principe est de définir des règles basées sur des ressemblances entre différents spams afin de les identifier de manière sûre. Il est possible de créer des règles très simples portant sur la présence d'un seul mot dans le corps d'un email : `/C1a11s/` ou bien de travailler sur des règles plus complexes `/(?:sck|l[i1]k).{1,3}(c[o0\.]c|d[i1|]c)/i`. Il est également possible de définir des règles portant sur des combinaisons d'expressions régulières ou bien de règles exploitant d'autres règles.

Les expressions régulières peuvent porter sur différents éléments du message, dont l'en-tête, le corps du message ou des éléments plus précis : URL contenus dans le message, message brut, contenu de pièces jointes... À titre d'information, l'antispam open-source Spamassassin utilise environ 800 règles (2900 pour Altospam).

Remarque : Il est conseillé lors de la diffusion de publipostages électroniques (*emailing*), de respecter les préconisations définies dans la RFC 2369. Le but de cette RFC est de définir des champs d'entêtes spécifiques aux *mailing-listes* pour préciser les URL ou adresses de désinscription notamment.

Listes noires et listes blanches

Il existe quatre types de listes : noires ou blanches, d'adresses IP ou de domaines. Les plus connues sont les listes noires d'adresses IP. Les listes d'adresses IP sont nommées : LHSBL (*Left-Hand Side based listing*) ou IPSBL (*IP based listing*) et celles de noms de domaine RHSBL (*Right-Hand Side*) ou HBL (*Hostname-based lists*).

Également couramment appelées RBL (*Realtime Blackhole List*) ou DNSBL (*DNS Black List*), les listes noires d'adresse IP sont des listes de serveurs connus pour aider, accueillir, produire ou retransmettre des spams ou fournir un service (relais ouvert) pouvant être utilisé comme support pour l'expédition de spam.

Les RBL peuvent être alimentées de plusieurs manières : spamtrap (pot-de-miel spécifique au spam), whois incorrectement configuré, logiciel antispam considérant les emails analysés comme des spams, dénonciation d'utilisateurs ou système automatisé de vérification de serveurs émetteurs.

La plupart de ces listes sont publiques, accessibles en consultation par tout le monde, certaines sont cependant privées. La RBL privée la plus utilisée est : *mail-abuse.com* (TrendMicro).

Le code de retour d'une requête de consultation de RBL est une

adresse IP. Pour spécifier la présence d'une IP dans une RBL, l'adresse habituellement retournée est : *127.0.0.2*. Certaines listes sont capables de renvoyer un résultat multivalué, pour cela elles utilisent des IP de retour de type : *127.0.0.<n>*.

La liste : *combined-HIB.dnsiplists.completewhois.com*, par exemple, est capable de retourner trois informations différentes. Dans ce cas précis : *127.0.0.2* indique que l'IP contrôlée appartient à un bloc IP non alloué et anormalement utilisé; *127.0.0.3*, l'IP appartient à un bloc IP détourné et *127.0.0.4*, l'IP appartient à un bloc IP invalide. Les principales RBL parmi environ 88 blacklists publiques à travers le monde (nombre en évolution permanente) sont:

bl.spamcop.net, combined.njabl.org, dnsbl.sorbs.net, list.dsbl.org, sbl-xbl.spamhaus.org, bl.csma.biz, combined-HIB.dnsiplists.completewhois.com, bulk.rhs.mailpolice.com. Les listes blanches sont exploitées par des sociétés commerciales qui accréditent la qualité d'un serveur de mail. Elles contiennent des sites, des domaines ou des adresses IP sûres et certifiées.

Parmi ces listes les plus connues sont : Habeas, Bonded Sender, SuretyMail (*ISIPP*). Il existe quelques listes, ni noires, ni blanches. Une liste spécifique répertorie tous les serveurs de Yahoo : *ybl.megacity.org* (attention cette liste n'est pas crédible). D'autres listes, plus utiles, permettent de connaître le pays d'origine de l'IP consultée : *tr.countries.nerd.dk, <PAYS>.blackholes.us*.

Les listes de domaines (RHSBL) sont utilisées et présentes sur Internet depuis moins longtemps. Elles sont cependant très utiles et permettent d'obtenir des retours d'analyse très intéressants. Elles peuvent être utilisées dans deux cas : soit pour contrôler le domaine expéditeur, soit pour vérifier les URL contenues dans un email. Dans ce dernier cas, souvent plus intéressant, une extraction des URL présentes dans le corps des courriers électroniques est effectuée pour vérifier chacune d'elles dans les RHSBL.

Sur un total d'environ 25 RHSBL existant actuellement, les principales et des plus utilisées sont : `rhsbl.sorbs.net`, `sbl.spamhaus.org`, `fulldom.rfc-ignorant.org`, `multi.surbl.org`, `multi.uribl.com`.

Remarque : Certaines blacklists proposées par `dnsbl.net.au` combinent des listes de domaines et des listes d'IP (attention l'utilisation de ces listes est limitée en nombre de requêtes).

Filtres Bayésiens

Le filtrage Bayésien est une méthode probabiliste de filtrage des courriers électroniques. Tirée des principes définis par Thomas BAYES, un mathématicien britannique du 18ème siècle, cette technologie fonctionne par apprentissage et se base sur une distribution statistique de mots clés présents dans les mails.

Deux bases sont créées (soit de manière manuelle, soit de manière automatique) : une première représentant des spams et une seconde des hams (messages légitimes). Le filtre analyse chaque mot représentatif d'un mail, en extrait par un calcul statistique sa probabilité de présence dans des spams et des hams. L'analyse sur l'ensemble du message permet d'obtenir un ratio global de probabilité qu'un email soit ou ne soit pas un spam.

Cette méthode est généralement une des rares technologies utilisées par les logiciels antispam installés sur les clients de messagerie (Thunderbird, Outlook, ...).

Elle a l'avantage de filtrer en fonction des besoins de chacun, elle nécessite cependant une période d'apprentissage. Elle donne également de très bons résultats sur des antispams centralisés, car un spam reste un spam, quel que soit le destinataire.

Bases collaboratives de spams

Ces bases de signatures de spams sont utilisées sur le même principe que les bases de signatures de virus mais sont alimentées automatiquement par leurs utilisateurs. Chaque système client calcule une signature numérique (un hash) pour chaque email reçu. Le

fait d'envoyer la signature permet d'alimenter la base de signatures et d'identifier ainsi les emails répétitifs (donc les spams). La comparaison de cette signature avec les serveurs décentralisés de la base collaborative, permet de classer l'email en lui affectant une probabilité d'être un spam.

Il existe essentiellement trois bases collaboratives de spams. Deux d'entre elles : *Razor* et *Distributed Checksum Clearinghouses* (DCC) appartiennent désormais à des sociétés privées. La dernière Pyzor est à l'origine d'une émanation OpenSource de *Razor*, qui a évolué de manière indépendante.

Systèmes d'authentification des emails

Il existe aujourd'hui plusieurs systèmes d'authentification d'émetteurs des emails. *Sender Policy Framework* (SPF), *Caller-ID* (Microsoft), *Sender-ID* (convergence de SPF et *Caller-ID*), *DomainKeys* (Yahoo) et DKIM (Yahoo et Cisco) sont des techniques ayant pour but d'identifier, pour un domaine donné, les hôtes autorisés à expédier des emails pour ce domaine.

Ces systèmes permettent d'apporter une crédibilité à l'émetteur d'un message. Le principe général est l'ajout d'un champ de type TXT sur le domaine émetteur soit pour définir la liste des serveurs émetteurs autorisés, soit pour publier une clé publique qui servira par la suite à authentifier l'émetteur d'un email.

SPF (Sender Policy Framework)

Cette technique est extrêmement simple, après extraction du domaine de l'émetteur (*MAIL FROM* : de l'enveloppe du message SMTP et non le champ *From* : de l'entête), une requête DNS de type TXT est effectuée sur le domaine en question pour connaître la liste des serveurs de messagerie autorisés à émettre des emails et pour la comparer avec l'IP émettrice du message.

La présence d'un champ TXT suivant : `domaine.tld IN TXT "v=spf1 mx ~all"` suffit, par exemple, à considérer que les serveurs émetteurs

d'un domaine correspondent à ses serveurs MX.

Pour définir simplement une adresse IP, utilisez la syntaxe : `v=spf1 ip4:192.168.0.1/32 ~all`.

Cette technologie possède cependant un problème concernant le *forwarding* d'email : dans ce cas le serveur émetteur ne sera pas forcément le serveur de messagerie de l'émetteur d'origine de l'email.

SenderID (Microsoft)

SenderID développé par Microsoft, est la convergence de SPF et *Caller-ID* (Microsoft). SenderID complète SPF en précisant que le champ *From* : de l'entête doit être vérifié en plus de l'adresse de l'enveloppe SMTP.

SenderID introduit la notion de PRA (*Purported Responsible Address*) permettant de déterminer l'adresse email responsable de l'envoi du message. Dans le cas d'*emailing*, par exemple, l'adresse d'émission de l'email et le responsable de l'émission peuvent être différents. SenderID propose également l'ajout de la commande *SUBMITTER* au protocole SMTP afin de résoudre les problèmes concernant le *forwarding* des messages.

DomainKeys (Yahoo)

Le principe de la technologie développée par Yahoo est de signer tous les emails émis avec une clé privée et de diffuser la clé publique correspondante via une entrée DNS afin que les serveurs destinataires puissent vérifier l'authenticité de l'email.

Les emails émis contiennent un champ d'en-tête supplémentaire nommé : *DomainKey-Signature* spécifiant différents éléments, dont l'algorithme de chiffrement utilisé (*a*), le domaine concerné (*d*), un sélecteur (*s*) et la signature du message elle-même (*b*). Le sélecteur permettant de travailler avec plusieurs clefs.

```
DomainKey-Signature: a=rsa-sha1
; q=dns; c=noews; s=s1024;
d=yahoo.com; h=X-YMail-
OSG:Received:Date:From:
Subject:To:Message-ID; b=cu
(...)CFjvazo;
```



Une requête DNS de type TXT sur l'entrée du sélecteur défini dans l'email (Cf. entrée s précédente) : `s1024._domainkey.yahoo.com` permet de retrouver les informations nécessaires sur la clé publique du domaine et de vérifier l'authenticité du mail :

```
"k=rsa;t=y;p=MIGfMA0GCsqGSI
(... )AB; n=A 1024 bit key;"
```

DKIM

DomainKeys Identified Mail (DKIM) est un draft (au sens IETF) issu de la fusion de *DomainKey* (Yahoo) et *Identified Internet Mail* (Cisco).

Tout comme *DomainKey*, DKIM spécifie comment signer les messages en utilisant un chiffrement asymétrique, en publiant les clés publiques via le DNS et en confiant le processus de signature aux serveurs de messagerie. La différence entre *DomainKey* et DKIM réside dans le fait que le signataire peut être différent de l'auteur et de l'émetteur, le champ de signature est auto-signé et la signature peut inclure un délai de validité.

Ces différentes technologies d'authentification sont cependant limitées. En effet, rien n'empêche un spammeur de configurer son serveur émetteur et son nom de domaine pour satisfaire également aux préconisations. D'autre part, ces technologies pourraient être une solution pour combattre le spam dans la mesure où tout le monde les utiliseraient. Or, la plupart des hébergeurs ne permettent pas l'ajout d'un simple champ TXT sur un domaine. Ces technologies n'ont donc comme seul but que de renforcer la lutte globale contre le spam et surtout de combattre le *spoofing* d'adresses email, mais elles ne protègent pas spécifiquement les utilisateurs.

Teergrubing

Le teergrubing est une technique proactive antispam consistant à maintenir une connexion SMTP ouverte longtemps. Le maintien de session SMTP a pour but de réduire significativement la vitesse de réponse du serveur émetteur sur certaines connexions considérées comme très

suspectes et d'éviter que le serveur de spam n'envoie pas de messages à d'autres destinataires.

Ainsi le teergrubing permet de contraindre le serveur de SPAM, malheureusement il contraint également le serveur qui implémente la technologie.

Greylisting

Le greylisting est une technologie antispam relativement récente qui consiste à rejeter temporairement un message, par émission d'un code de refus temporaire (code 4xx) au serveur émetteur. Le serveur émetteur légitime réexpédie le mail quelques minutes après, il respecte ainsi les préconisations définies dans la RFC SMTP. Par contre, la plupart des serveurs de spam ne prennent pas cette peine !

Pour conserver l'information de tentative d'émission par le serveur, un triplet identifié par l'adresse IP du serveur émetteur, l'adresse email de l'expéditeur et l'adresse email du destinataire, est associé à chaque mail entrant. Ainsi, si le triplet apparaît pour la première fois, le serveur de messagerie renvoie un code de refus temporaire au serveur SMTP distant et sauvegarde l'information.

Si le triplet réapparaît après un certain temps (prévoir entre 15 minutes et une demi-heure) le message est accepté et notre triplet est whitelisted. Une réinitialisation de triplets whitelisted est à prévoir afin d'éviter tout abus. Il existe malheureusement des imperfections à l'utilisation de cette technologie. L'utilisation du greylisting créé un temps de latence entre l'expédition du message et sa réception par son destinataire lors des premiers échanges ou après les réinitialisations.

En outre, de par son fonctionnement, les messages sont reçus plusieurs fois par le serveur de messagerie destinataire ce qui peut le saturer et encombrer la bande passante. D'autre part, certains serveurs de spams sont capables de passer outre cette technologie en réémettant périodiquement les spams non délivrés.

Pour éviter ce type d'inconvénient, une alternative consiste à combiner le greylisting aux solutions standards de filtrage de spams. L'intérêt d'une telle combinaison est de ne greylister que les messages difficilement identifiables comme des spams.

Ainsi, les messages licites seront directement reçus par leurs destinataires, les spams identifiés de manière sûre seront refusés et les emails prêtant à confusion devront passer le test de greylisting.

Analyse des images

Suite à l'augmentation du nombre de spam-image, il est devenu nécessaire d'intégrer un système d'analyse des images contenues dans les emails. Cette analyse peut porter sur différents procédés :

- Comparaison des caractéristiques des images (nombre d'images, nom, format et dimensions des images, taille des fichiers) avec les caractéristiques couramment rencontrées dans les spam-image.
- L'utilisation de techniques de reconnaissance de caractères (OCR) permet une analyse des images. Cependant, bien que les techniques de reconnaissance de caractères soient performantes, son utilisation pour extraire les mots clés d'une image est peu probante. Les traitements sont consommateurs en ressources CPU et les spammeurs ont déjà contourné la détection en utilisant des images animées, en décalant les caractères et en intégrant des signes afin de gêner la reconnaissance.
- Une étude portant sur l'analyse d'image par découpage et apprentissage via l'utilisation d'un système de *Datamining* a été expérimentée par le cabinet HSC. D'après eux, les résultats sont intéressants mais le système est très consommateur en ressources machine.

Etant donné la fiabilité et les performances des résultats obtenus par

les OCR, il est plutôt recommandé aujourd'hui d'effectuer une analyse des images basée sur l'analogie avec la topologie des spam-image.

Test de Turing

Cette technique, également nommée challenge/réponse, consiste à authentifier l'expéditeur d'un email afin de s'assurer de son existence physique via une demande d'authentification envoyée à l'expéditeur. Une fois un code (affiché dans une

image) reproduit, le message est acheminé au destinataire.

Utilisé séparément, ce type de solution ne fait que déporter la problématique du spam sur l'expéditeur du message et présente un grand nombre d'inconvénients :

- Les spameurs utilisent généralement des adresses email usurpées à des utilisateurs légitimes. Ces derniers reçoivent alors des emails, non sollicités,

de confirmation d'authentification sans avoir été à l'origine de quoi que ce soit.

- Ce type de solution nécessitant une action humaine génère un nombre important de faux-positifs (newsletters, utilisateurs ne souhaitant pas perdre de temps ou contre le principe, système d'alerte ou de *monitoring*, ...).
- Des problèmes de fonctionnement ont également été mis en avant dans le cas où deux interlocuteurs utilisent des systèmes équivalents : un *ping-pong* récurrent se met en place pour une demande réciproque d'authentification.
- D'autre part, certains spameurs, notamment dans le SCAM (Nigérian 419), prennent le temps de s'authentifier auprès de ces systèmes.

Il est cependant extrêmement intéressant d'utiliser cette technologie uniquement en cas d'analyse négative par les technologies standards (si le mail est considéré comme un spam).

Cela permet en dernier recours de pouvoir éviter les éventuels derniers faux-positifs que l'analyse automatisée pourrait générer.

Conclusion

Chacune de ces technologies prise séparément ne permet pas d'obtenir des résultats satisfaisants, elles possèdent toutes des avantages et des inconvénients propres.

Cependant, ces technologies basées sur des éléments différents permettent, assemblées de manière judicieuse, d'obtenir des performances d'analyse très intéressantes.

La combinaison de techniques comme le greylisting et/ou le test de Turing avec des techniques plus classiques permet à la fois d'obtenir des filtrages de grande qualité mais permet surtout d'arriver à un taux de faux-positifs extrêmement bas. ●

Terminologie

- DCC : Distributed Checksum Clearinghouses,
- DKIM : DomainKeys Identified Mail,
- DNSBL : DNS Black List,
- FQDN : fully qualified domain name (nom complet du serveur),
- HBL : Hostname-based lists (idem RHSBL),
- IPBL : IP based listing (idem LHSBL),
- LHSBL : Left-Hand Side or IP-based listing (listes d'IP),
- RBL : Realtime Blackhole List (liste noire),
- RHSBL : Right-Hand Side or Hostname-based lists (liste de noms de domaine),
- SCAM ou Nigeria 419 : Cyber-arnaque abusant de la crédulité des gens pour leur soutirer de l'argent,
- SPF : Sender Policy Framework.

À propos de l'auteur

Ingénieur informaticien de formation, Stéphane Manhes a 8 ans d'expérience dans le domaine de la sécurité informatique en tant que consultant et expert. Stéphane Manhes est responsable du service de protection de la messagerie Altospam pour la société Oktey. Altospam intègre un système d'analyse des emails basé sur une combinaison de 14 technologies antispam complémentaires.

Sur Internet

- http://fr.docs.yahoo.com/mail/spamguard_domainkeys.html – DomainKey,
- <http://projects.puremagic.com/greylisting/whitepaper.html> – Greylisting,
- <http://pyzor.sourceforge.net/> - Pyzor,
- <http://razor.sourceforge.net/> - Razor,
- <http://www.altospam.com/> - Antispam basé sur une combinaison de 14 technologies complémentaires,
- <http://www.dkim.org/> - DKIM,
- <http://hsc.fr/ressources/presentations/sl2007-spam-image/> - Etude HSC,
- <http://www.ietf.org/rfc/rfc2821.txt> - RFC Simple Mail Transfer Protocol,
- <http://www.iks-jena.de/mitarb/lutz/usenet/teergrube.en.html> – Teergrubing,
- <http://www.microsoft.com/mscorp/safety/technologies/senderid/> - SenderID,
- <http://www.openspf.org/> - SPF,
- <http://www.rhyolite.com/anti-spam/dcc/> - DCC.