



HERVÉ SCHAUER CONSULTANTS

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

## *Solutions Linux Paris 2005*

# Méthodes anti-spam

**Denis Ducamp**  
<Denis.Ducamp@hsc.fr>



- Aujourd'hui il est demandé à un seul relais de messagerie d'assumer de nombreuses fonctions :
  - relayage SMTP sécurisé, anti-virus et anti-spam
- Pour cela il est en fait nécessaire de combiner plusieurs briques.
- Si l'anti-virus permet de protéger les postes clients
  - L'anti-spam n'est présent que pour permettre aux utilisateurs d'utiliser au mieux leurs boîtes à lettres
  - C'est-à-dire retrouver rapidement les 5 mails légitimes parmi les 150 spams
  - Ce qui reste possible même si 10% des spams ne sont pas marqués.
- De nombreuses méthodes anti-spam existent
  - Beaucoup n'ont pas été conçues pour cela et sont donc détournées
  - Certaines ont été conçues pour cela mais abusent des ressources des autres.

- Listes noires
  - Locales et DNS (d'adresses IP et de domaines)
- Bases de signatures
- Bases de spams
  - Razor, Pyzor et DCC
- Authentification des relais sortant
- Auto-whitelist
- Bayes
- Callbacks
- Challenge / réponse
- Greylisting

- Listes gérées par l'administrateur du serveur
- Permet d'interdire les connexions
  - Depuis des adresses IP spécifiées
  - Depuis des adresses IP de certains domaines
  - Utilisant certains HELO/EHLO
  - Utilisant certains MAIL FROM:
  - Utilisant certains RCPT TO:
- Travail solitaire
  - Demandant beaucoup de ressources
  - Et pouvant facilement générer des faux positifs

- Une DNSBL est une Black List DNS :
  - Toutes les adresses IP que le serveur connaît sont suspectes
- Les natures des adresses IP peuvent différer :
  - Adresses IP d'où des spams ont été envoyés
  - Adresses IP de relais ouverts sur Internet (SMTP, HTTP, socks, telnet...)
  - Adresses IP de clients de FAI sur des plages d'adresses dynamiques
  - Etc.
- Les politiques de gestion de ces listes diffèrent :
  - Modalités d'entrée/sortie, réactivité, etc.
- Aussi bien les serveurs SMTP que les logiciels anti-spam peuvent utiliser des DNSBL
  - Mais les serveurs SMTP ne permettent pas les faux-positifs
- Site de test : <<http://www.dnsstuff.com/>>
- Listes de DNSBL : <<http://www.moensted.dk/spam/>> et <<http://www.declude.com/junkmail/support/ip4r.htm>>

- Des serveurs connaissent des listes de domaines suspects
- Les natures de ces domaines peuvent différer :
  - Domaines de spammeurs
  - Domaines mal configurés
  - Domaines de sites utilisant le spam comme moyen marketing
  - Etc...
- Les politiques de gestion de ces listes diffèrent :
  - Modalités d'entrée/sortie, réactivité, etc.
- Ces données peuvent être comparées
  - Aux domaines des serveurs clients et/ou du MAIL FROM:
  - Aux domaines cités dans les mails
- Aussi bien les serveurs SMTP que les logiciels anti-spam peuvent utiliser des DNSBL
  - Mais les serveurs SMTP ne permettent pas les faux-positifs

- Comme dans le cas des anti-virus
  - Une base de signatures est construite à partir de spams connus
  - Mais pour ne détecter que certaines particularités
- Or tout le monde peut utiliser ces particularités
  - Exemple : *newsletters* ressemblant à des spams pour le V\*\*gr\*
- Chaque signature est alors pondérée
  - Et un message est considéré comme un spam si un seuil est atteint
  - Les pondérations doivent être calculées pour minimiser les faux-positifs
- Plusieurs problèmes se posent :
  - Pour diminuer les faux positifs, des règles détectent des messages licites
    - Ces règles sont facilement abusées par les spammeurs : donc à éviter absolument
  - Il faut mettre à jour ces bases régulièrement
    - Toute modification peut demander à changer significativement les pondérations

- L'utilisation des ressources réseaux, dynamiques par nature, permettent de faire contrepoids aux bases de règles statiques.
- Il peut être possible d'utiliser des bases de règles générées par d'autres personnes
  - Par exemple pour SpamAssassin, le script `my_rules_du_jour` permet de télécharger plusieurs listes de ce type :  
<<http://www.exit0.us/index.php/RulesDuJour>>
- **ATTENTION** : il est important de vérifier que des jeux de règles tiers utilisés ne génèrent pas de faux positifs
  - pour cela il faut essayer ces règles sur deux corpus de hams et spams, représentatifs des mails reçus et datant de moins de 6 mois
  - les raisons des faux positifs avec l'utilisation de nouvelles règles sont :
    - que les scores du nouvel ensemble de tests n'ont pas été recalculés en incluant les nouvelles règles
    - les corpus de hams utilisés pour tester les nouvelles règles sont souvent non significatifs des hams reçus par des tiers.

- Des bases de spams sont confectionnées de façon collaborative
  - Grâce à la collaboration de ses utilisateurs.
- Chaque (partie de) message reçu(e) est comparé(e) à une base centrale
  - Entre le « client » et le « serveur central » seuls des « hashes » sont échangés.
- Certains systèmes permettent de détecter des spams « mutants ».
- Certains systèmes utilisent un « niveau de confiance/spammicité ».
- De telles bases sont Razor, Pyzor et DCC.
  - Ces systèmes sont plus souvent utilisés par un logiciel anti-spam
  - Mais peuvent être utilisés par les serveurs SMTP

- Razor est une base de spams
- Le client, écrit en perl, est OpenSource
  - Le serveur n'est pas OpenSource et géré par un comité restreint
- La version 1 de razor, de moindre confiance dans son mode de fonctionnement, n'est plus supporté.
- La version 2 ajoute un niveau de confiance dans ses collaborateurs
  - Il est difficile d'avoir un bon niveau de confiance
  - Il est facile de le faire chuter
  - Ce qui permet de contrer les attaques contre certaines listes de diffusion
- Une nouvelle signature, `Whiplash`, permet de détecter les URL de sites qui utilisent le spam pour faire de la pub.

- Pyzor est une implémentation OpenSource de Razor
- Il possède malgré tout son propre protocole client/serveur.
- Il est possible de s'installer son propre serveur
  - Qui peut alors servir de base et/ou de cache locaux
- Le mode de fonctionnement de Pyzor correspond à celui utilisé dans la version 1 de Razor.
  - La base pourrait donc être abusée

- DCC est un système de comptabilisation d'occurrences de sommes de contrôles des mails reçus
  - plus le nombre de destinataires est grand et plus les présomptions sont fortes.
- Les sommes de contrôle utilisées permettent de détecter les spams personnalisés / « mutants ».
- Il est possible de s'installer son propre serveur
  - pour l'utiliser de façon isolée
  - pour l'utiliser comme un cache local interrogeant les serveurs officiels
    - méthode conseillée au delà de 100.000 messages par jour.
- Sur un serveur SMTP, DCC est généralement couplé à un système de greylisting

- Plusieurs méthodes permettent "d'authentifier" les serveurs sortants
  - N'accepter des mails que depuis les serveurs sortants du domaine de l'expéditeur
  - Par exemple : *SPF* publie par DNS les serveurs autorisés
- Certaines fonctionnalités peuvent être "cassées"
  - Comme le *.forward* et les alias
  - Et nécessite d'autres fonctionnalités pour les "réparer"
    - Par exemple : *SRS (Sender Rewriting Scheme)* peut "réparer" *SPF (Sender Policy Framework)*
- Systèmes à utiliser de préférence sur les serveurs SMTP
  - Les logiciels anti-spam pouvant être perturbés par des enveloppes modifiées et/ou des entêtes additionnelles.
- Méthodes non conçues pour lutter contre le spam
  - Les spammeurs ont fait partie des premiers utilisateurs de *SPF*.

- Base dynamique enregistrant pour chaque expéditeur :
  - Le nombre de mails reçus
  - La moyenne des scores des mails reçus
- Pour chaque nouveau message
  - Un score est ajouté pour tirer le score vers la moyenne de l'expéditeur
- Permet
  - Qu'un gros spammeur soit toujours détecté
  - Qu'un mail d'une personne connue ne soit pas détecté comme un spam
    - Même si elle fait suivre de petits spams.
- Système à utiliser dans un logiciel anti-spam ou sur le poste client

- Base dynamique enregistrant des statistiques sur les mots contenus dans les mails
  - Chaque (suite de) mot(s) est associé(e) à un nombre d'occurrences dans les spams et dans les hams.
- Un score est associé suivant que les (suites de) mots les plus courant(e)s du mail
  - Occurrent le plus souvent dans des spams ou dans des hams.
- Permet de classifier les messages en deux catégories : spams/hams
- La base doit être alimentée avec un certain nombre de mails
  - Pour qu'elle puisse être utilisable
  - Puis doit être mise à jour avec toutes les erreurs qu'elle commet.
- Méthode à privilégier sur le poste client
  - Chaque utilisateur a sa propre définition du spam
  - Et est directement confronté aux erreurs commises par ce système

- Base dynamique enregistrant les correspondants existants
- Quand le serveur SMTP a reçu l'enveloppe d'un message
  - Il forge un message qu'il tente d'envoyer à l'expéditeur
    - Sans envoyer de partie DATA
  - Si ce "message" est refusé alors le message initial est refusé
    - Car un `bounce` ne pourrait être envoyé en cas d'erreur
  - S'il est accepté alors la transaction SMTP initiale continue
- Méthode qui utilise les ressources d'autres serveurs
  - Notamment lorsque les spammeurs usurpent une adresse existante
  - Il est possible de limiter cet usage à des domaines qui sont notoirement connus pour être usurpés
    - tant qu'ils n'ont pas mis en place de méthode d'authentification

- Base dynamique enregistrant les correspondants légitimes d'un utilisateur
- Quand un mail avec un expéditeur inconnu est reçu
  - Le mail est mis en quarantaine
  - Le système envoie un challenge à l'expéditeur
  - L'expéditeur doit renvoyer le challenge
  - À la réception du challenge
    - Le système accepte le nouveau correspondant comme légitime
    - Envoie à son destinataire les messages de cet expéditeur.
- Les spammeurs forgent souvent les adresses sources
  - Les victimes reçoivent en plus des avis de non distribution
  - Les challenges de ces systèmes.

- Base dynamique enregistrant les triplets déjà rencontrés
  - Adresse IP source, MAIL FROM:, RCPT TO:.
- Lorsque l'enveloppe a été envoyée au serveur :
  - Si le triplet n'a jamais été vu alors
    - Le triplet est enregistré et une erreur temporaire est retournée au client
    - Si le triplet a déjà été vu alors la transaction SMTP initiale continue
- Permet de refuser des mails de serveurs SMTP non conformes
  - Qui ne ré-émettent pas les messages qui n'ont pu être envoyés à cause d'une erreur temporaire.
  - Principalement les zombies installés sur des postes vérolés sur Internet
- Système à utiliser sur les serveurs SMTP
- Nécessite une administration de tous les instants pour accepter
  - Les "serveurs" mal conçus, par exemple des CGI qui envoient eux-même des mails
  - Les serveurs hébergeant des listes de diffusion avec VERP.

- À vous de choisir les méthodes à utiliser
  - La performance n'est pas le seul paramètre à prendre en compte
- Plus le serveur SMTP effectue de tests
  - Plus les messages seront rejetés tôt
  - Mais plus les performances seront faibles
  - Et les ressources nécessaires élevées
    - Notamment lors d'ajouts de tests dans les enveloppes
  - Attention : les faux positifs sont définitifs au niveau du serveur SMTP
- Un logiciel anti-spam peut combiner plusieurs résultats
  - Permettant de mitiger les risques de faux positifs
  - Mais certaines méthodes sont limitées (SPF) ou impossibles (Greylisting)
- Il vaut mieux limiter certaines méthodes au poste utilisateur (Bayes)
  - Faut il encore former l'utilisateur...

- Car rien ne remplacera une personne bien informée :

- [http://www.admi.net/cgi-bin/wiki?Lutte\\_Contre\\_Le\\_Spam](http://www.admi.net/cgi-bin/wiki?Lutte_Contre_Le_Spam)

- avec des actualités,
- des liens et ressources,
- des initiatives professionnelles et
- des organismes de lutte contre le spamming

- <http://caspam.org/>

- CASPAM - Collectif Anti Spam

- avec « 6 choses a faire ou ne pas faire pour lutter contre le spam !! »

- [http://www.cnil.fr/thematic/internet/spam/spam\\_sommaire.htm](http://www.cnil.fr/thematic/internet/spam/spam_sommaire.htm)

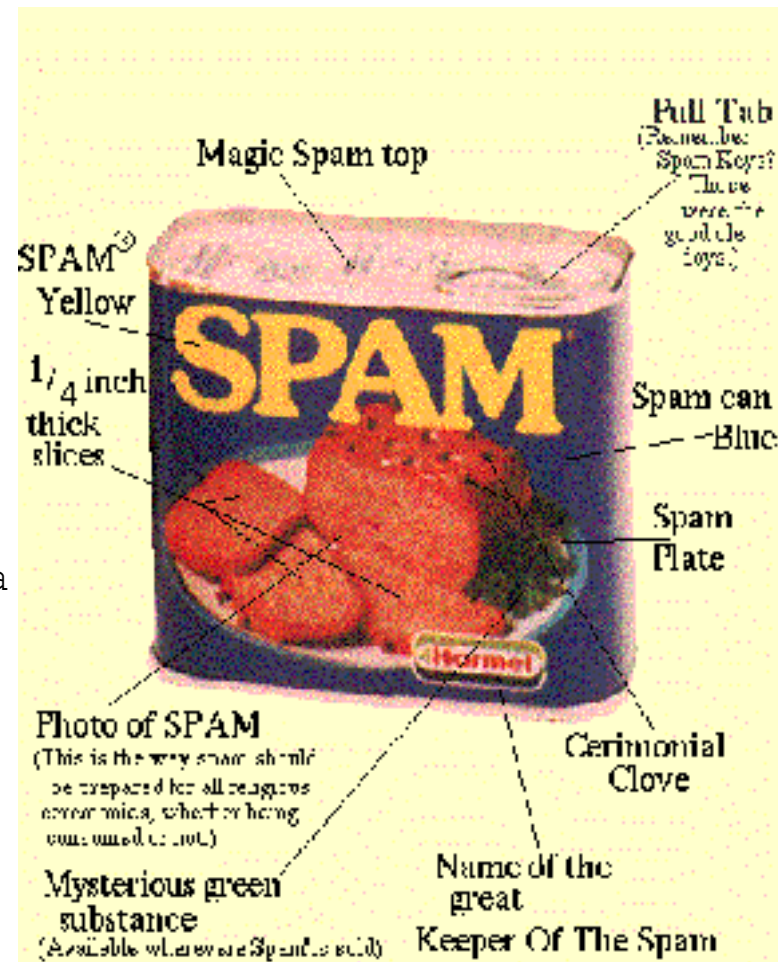
- CNIL - Halte au spam

- avec « comment se prémunir ? »

- <http://www.hoaxbuster.com/>

- Première ressource francophone sur les hoax

- les derniers canulars circulant sur le réseau.



<http://www.physics.upenn.edu/~pcn/spam.gif>

N'hésitez pas à poser vos questions...

et à venir visiter notre site WEB : <http://www.hsc.fr/>

pour y lire nos autres présentations sur le même sujet :

- Éléments de réflexion sur le spam

<http://www.hsc.fr/ressources/presentations/ddmspam/>

- Spamassassin

<http://www.hsc.fr/ressources/presentations/spamassassin/>

- Serveur de messagerie sécurisé et libre

<http://www.hsc.fr/ressources/presentations/SrvMessagSecLib/>

et sur bien d'autres sujets de sécurité...

Merci de votre attention

Et n'hésitez pas à me poser vos questions...

...sans réveiller ceux qui se sont endormis ;-)