



de Tésor® Computers optez pour la sécurité

Rue du Centre, 57 • B-4800 Verviers • BELGIUM • Tél. +32 (0)87 293 770 • Fax. +32 (0)87 293 509 • mail : info@detesor.be
Nouvelle Adresse : 100 Louvain • Proximité : 5 • B-4019 Diegem • BELGIUM • Tél. +32 (0)87 293 473 3 • Fax. +32 (0)87 293 473 20

Halte au Spam !

Etat des lieux & solutions.

Jean-Paul Rosette
jean-paul.rosette@detesor.be
Tél. (087) 293 770
de Tésor Computers SA
Solutions informatique pour entreprises
Verviers & Diegem



Qu'est-ce que le spam ?

- Un pâté de porc en boîte ?
(1937 - Spice Ham – Corned-Beef)
- Un courrier indésirable ?
- Une énorme perte de temps ?
- La porte ouverte aux escrocs ?
- Une source de nuisance ?
- **TOUT CELA A LA FOIS !**





Pourquoi le terme SPAM ?



Episode 12 de la première série (années '70) réalisée par les *Monty Python's Flying Circus* pour la télévision britannique. Un serveur n'avait rien d'autre à proposer que du *Spam* ...
> Mauvais et bruit de fond 🗣️ 🗣️



Essayons de définir le Spam ...

Il s'agit d'un e-mail (mess. Instan., sms, ...)

- d'exemplaires identiques
- envoyé en masse (bulk e-mail) ... *mailbombing*
- de façon automatique
- au contenu non sollicité, non désiré et non pertinent
- envoyé sans mon plein consentement
- Essayant d'apparaître comme un message classique et valide



En bref, le Spam c'est ...

- *Le spam, c'est tout le courrier que vous recevez de parfaits inconnus, de Richard, qui vous propose aimablement d'agrandir votre pénis de plus de 35 cm, de Scott qui, lui, veut vous faire gagner de l'argent gratuitement en restant le cul posé sur votre chaise, tout ce que vous avez à faire, c'est de lui donner votre numéro de carte de crédit. Katia, beaucoup plus élégante, s'inquiète de votre santé et veut vous vendre des pilules qui vous feront vivre jusqu'à 15 ans de plus ! Merci c'est touchant toute cette attention, n'est-ce pas ? Mais, tout ça, c'est du courrier à traiter et qui occupe de la bande passante. Et, de plus, vous risquez de passer à coté d'un message important (la commande de votre vie!) perdu dans tout ce fouillis anglophone !*



SPAM - Définition

Unsolicited bulk e-mail, junk mail, pourriel ou spam

Cela signifie que :

- Le destinataire n'a pas la possibilité d'arrêter la réception de futurs messages provenant du même expéditeur et / ou
- Le destinataire n'arrive pas à établir une relation entre lui-même et l'expéditeur.

Giga Research, Fighting Spam Today and tomorrow

... et pour nous rendre la tâche encore plus difficile, il est souvent très délicat de faire la distinction entre un spam et un message valide !



Le Spamming est relativement facile

- Il est simple de mentir au sujet de l'identité de l'utilisateur ou du serveur
- Il est simple de contrefaire (ou maquiller) le protocole e-mail (SMTP = SIMPLE Mail Transport Protocol) *FTP modifié 1973*
- Transférer un e-mail d'un ordinateur (server) à un autre est une des caractéristiques principales du mail
- Retracer la vraie route vers un expéditeur est difficile
- De grands intérêts économiques sont en jeu et le commerce on-line a le vent en poupe



La “Spam-économie” & les “cybermafieux”

- Cela ne coûte quasi rien d'envoyer du Spam. Même si le taux de réponse est inférieur à 0.1 %, un spammer peut gagner \$10,000 en ayant envoyé 10 millions de messages pour un produit avec une marge bénéficiaire de \$1.
 - Si un spammer atteint un taux de réponse de 1% (beaucoup se vantent de l'atteindre), les gains peuvent alors atteindre \$100.000 !

• Dans un article récent du Wall Street Journal, une dame prétendait qu'elle faisait déjà du profit avec 100 réponses par 10 millions de messages envoyés ! Toujours d'après elle, ses revenus 2003 ont d'ailleurs atteint \$200,000 net !

D'après www.spamhaus.org, 200 personnes seraient responsables de 90 % du spam que nous recevons. (clubs, activités criminelles, virus, trojan, ...)



Comment procède le spammer ?

- Vendre un produit quelconque
- Trouver un client qui a qqchse à vendre (% ou forfait)
- Trouver un client qui désire du trafic (porno ou casino)
- + original : petites actions boursières
- Pyramide, demande d'argent, fraude à la carte, Nigéria, ...



La collecte d'adresses

Les adresses e-mail valides sont faciles à collecter

- Les sociétés et organismes divers vendent souvent des listes officielles. Les spammers vendent aussi leur liste: 200 millions de mails pour 29,95 \$!
- Les utilisateurs postent leur e-mail dans les newsgroups, dans les "pages jaunes", sur les sites commerciaux, ...
- Présence de l'adresse e-mail "en clair" sur un site ou sur votre site commercial. (Robot - solution: adresse munging)
- Le harvesting (brute force attack) est facile à réaliser et permet la récolte de milliers d'adresses e-mail valides (aaa@societe.be, ...) ou attaque dictionnaire
- Pillage de votre (ou d'un) carnet d'adresses d'un PC infecté par un spyware ou trojan – cc - Intrusion et vol d'e-mail

** Un spammer a mené une attaque géante (dictionnaire) contre les serveurs des célèbres messageries Hotmail.com et MSN.com, à un rythme de 3 ou 4 essais par seconde, 24 heures sur 24, et cela, continuellement pendant les 8 derniers mois.*



Les petits 'trucs des spammers'

- Fausse réponse Re:
- Faux message égaré avec un ton amical et vantant un produit ou un service
- Fausse confirmation d'abonnement, de commande, d'envoi, ...
- Adresse surprise de type
`http://%59%57%36%33.%74%6b` > site porno
- Message avec véritables adresses e-mail en cc:
- Message envoyé par vous-même !
- Message en HTML pour éviter les anti-spam



Le vol de votre adresse - Conclusion

Plus votre adresse e-mail est visible, plus elle est spammée !

> Les adresses présentes sur des sites à contenu 'sexuel' sont encore plus spammées.



Le talon d'Achille des spammeurs

Mise en place d'un site Web & envoi des messages

- Fournisseurs d'accès local
- Son propre serveur (aussi connecté à un FAI)
- Serveur basé dans des pays avec FAI *tolérants (bullet-proof ou blindé)*
- *Serveurs de type Open-Relay (ouverts ou mal configurés) avec l'avantage d'un quasi anonymat du spammer*
- *Ordinateurs contaminés. (500.000 à plusieurs millions dans le monde) 'Zombies' ou 'fresh proxies'. D'où, gratuité et anonymat! Etude parle de 50 à 80 % des spams envoyés ...*

Problème de temps ! De quelques heures à quelques jours mais cela s'avère suffisant pour gagner de l'argent



Protéger votre adresse e-mail

Les solutions pour limiter la collecte de votre adresse

- Déguiser son adresse. Ex: *nom at societe point com, n0m@s0ciete.c0m (remplacer les zéros), image, codage JavaScript, formulaire de contact (PHP, ASP), 'écrivez-moi', ... (robot avec l'aide de Google)*
- Utiliser différentes adresses e-mail. *nom@hotmail.com*
- Privilégier les adresses assez longues ou complexes *fiyh56a*
- Bien lire les conditions commerciales des sites.
- **Ne jamais répondre** à un e-mail de spammer et ne pas tenter de se désabonner
- Ne pas répondre aux chaînes e-mail. (charité, cc, cci, ...)
- Ne pas transférer les chaînes de messages (hoax, ...)
- Mettre à jour vos logiciels (OS, messageries, anti-virus, firewall, ...)



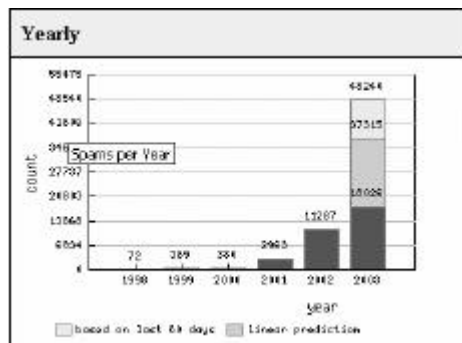
Spam – Les nuisances

- Encombre les infrastructures
- Perte de productivité, perte d'attention et perte de messages utiles !
- Temps de téléchargement, ralentissements et blocage ...
- Sécurité (contient virus, malware, ...)
- Expose les utilisateurs à la pornographie
- Risque juridique (spam-relay, ...)
- Suppression des messages valides et même risque d'abandon de l'e-mail !



SPAM – The Cost To Business

- Le Spam représente désormais + de 50 % des mails que reçoivent les entreprises et cela continue à augmenter.
- Et il n'y pas d'arrêt ou même de ralentissement en vue !



*Source: Bloodgate.com

En 2003, le Spam a coûté au business américain plus de \$10 milliards.



SPAM – The Cost To Business



Le spam et la loi

- **Opt-in**
Accord explicite
Principalement Europe (Directive 2002/58/EC)
et Australie.
Belgique (mars 2003), GB: opt-in uniquement pour les particuliers.
- Double opt-in: e-mail de confirmation pour les vrais e-marketer
- **Opt-out**
Sans accord préalable et possibilité de refus
Etats-Unis (*Can-Spam 1/1/2004: Controlling the Assault of Non-Solicited pornography and Marketing*) et la plupart des pays asiatiques.
Adresse, désinscription, pas de robot, pas de falsification, amendes 3M\$ & 5 ans,
...

*Le spam vient directement ou indirectement des USA !
(Relais: Chine, Russie, Brésil, 'Corée du sud', ...)*



Autopsie d'un e-mail

- **Sélectionnez le mail dans votre boîte de réception, puis "Affichage des propriétés" ou du "Source de la page" »**

Received: from blabla15.blabla.com [190.21.56.47] --> (1)
by smtp.votre-fai.com with ESMTP (SMTPD32-4.06) id A09D3203BC;
Tue, 05 Jan 1999 13:57:33 EST
Received: from argamemnon ([192.249.17.1]) --> (2)
by blabla15.blabla.com (8.7.5) ID LAA28548; --> (3)
Tue, 5 Jan 1999 11:56:11 -0700 (MST)
Message-ID: <007901be38dc5e19a50e0\$01010118@argamemnon> --> (4)
Reply-To: billgates@microsoft.com --> (5)
From: zorro@masque.com --> (6)
To: votre-adresse@votre-fai.com --> (7)
Subject: Visitez mon site !!! --> (8)
Date: tue, 5 Jan 1999 19:54:10 +0100
MIME-Version: 1.0
Content-Type: text/plain;
charset="iso-8759-2"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 4.72.3110.5 --> (9)
X-MimeOLE: Produced By Microsoft MimeOLE V4.72.3110.3
X-UIDL: 568
Status: U

- (1) adresse IP du serveur par lequel a transité le spam
(2) adresse IP du spammer
(3) serveur SMTP utilisé par le spammer
(4) nom réseau de l'ordinateur du spammer
(5) adresse où sera acheminée votre réponse éventuelle
(6) adresse présumée du spammer (peut avoir été supprimée ou falsifiée)
(7) votre adresse email
(8) objet du mail
(9) logiciel de mail utilisé par le spammer



Le spam – Solutions & techniques

- Solution anti-virus et anti-spam ou solution intégrée hard & soft du même éditeur.
- Black lists ou listes noires (Realtime Blackhole Lists) > abonnement annuel. (IP 212.123.14.83)
- White lists ou listes blanches. Adresses et domaines sûrs. Automatique dans le soft.
- Listes grises. Refus systématique de tous les e-mails. 'Challenge-Response'
- ...



Le spam – Solutions & techniques

- Filtres bayésiens basé sur les probabilités.
 - 1) Tous les messages analysés
 - 2) Création BD avec mots 'valides' et 'spam'
 - 3) Distribue ou arrête mail

> souvent associé à des algorithmes complexes: mots modifiés, mots dans des images
- *Subterfuge : envoi d'un avis de 'non remise' du courrier à l'intention du spammer.*



4 options de déploiement.

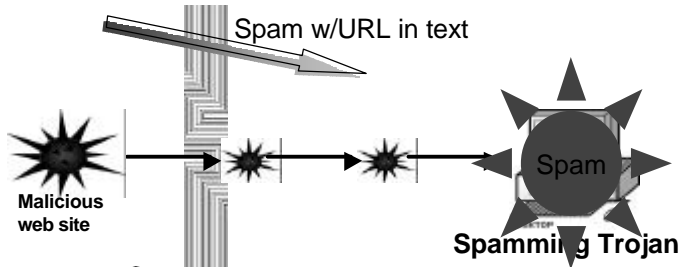
Avant > Analyse du coût du spam !

- Petites structures : soft anti-spam sur chaque poste. (bon marché, MàJ par poste, maintenance complexe)
- Add-on sur le serveur mail. (Compatibilité avec Exchange, Lotus Notes, ...)
- Passerelle (gateway) spécialisée (edge ou DMZ) entre firewall et réseau. (soft sur serveur, appliance, serveur dédié open source, ...)
- Hébergement externe avec anti-spam.



SPAM, Control Filtering et anti-virus

Anti-spam sol. will block this via SMTP



Spam-only n'arrêtra pas le chargement de ce Trojan

Spam-only n'empêchera pas l'utilisateur de visiter ce site



Référence aux base de données Similaire aux bases de signatures des anti-virus

"J'ai déjà vu ce message et c'est du spam"



Les tactiques des spammers pour contourner

- Génération random de caractères – insertion tant dans le *header* que dans le *body*
- Text paragraph re-sequencing
- Single use 'From' address – no recycling

- 1 - Les 'Honey Pot' sont populaires sur Internet. Ils reçoivent un maximum de spams
 - 2 - Ces spams sont transférés dans un centre où chaque message est visionné par un humain
 - 3 - Les spams sont référencés par une *hash pattern* (signature) unique et stockée dans une database
 - 4 - Les mises à jour sont envoyées très régulièrement vers le client utilisateur (vous)
 - 5 - Chaque message qui arrive dans votre messagerie est *hashed* et sa signature est comparée à la base
- Problème : Inutile contre les premiers spams



Solutions - Lexical Scanners Technique de base des anti-spam standards

"Ces mots indiquent du spam"

2

Techniques des spammers pour contourner

- Encodage HTML

- HTML comments inserted to split words

- Mauvaise orthographe (cialis), ajout d'espaces dans les mots (via gra), ou remplacement des lettres par des nombres (v1agra)

- 1 - L'administrateur configure le Content Policy server in le mail server
- 2 - Le serveur est configuré avec pre-defined lexicons of keywords qui indique le spam
- 3 - L'administrateur peut modifier lexicon, basé sur sa propre configuration
- 4 - Le serveur analyse le message texte, performs disposition

Problème : risque de faux positifs surtout si beaucoup de règles sont activées



Analyse du header (script) Identification de la source de l'e-mail

"Cette entête SMTP (header) indique du spam"

Spammer tactics to avoid detection by header analysis

- Not suppressing SMTP: From

- Sending to single recipient

- Frequently changing IPs within Net block

- 1 - Admin recherche les sources anti-spam scripts and les ajoute sur the Internet
- 2 - Scripts added to the mail server through MTA APIs
- 3 - Header pour le spamming email analyzed
- 4 - Disposition performed, based on further Admin scripting

Les solutions anti-spam basées sur les RBL (Relay Black Lists, spamhaus.org, spamcop.net) utilisent cette approche.



Pourquoi le filtre heuristique ?

Proactive Heuristics Technology Performs Better Than Reactive Database/Fingerprint Technology

- Reactive, database/"fingerprint" products identify spam that they have seen before
 - Since more and more spam is "first time" or altered spam, the effectiveness of the reactive anti-spam products have diminished
 - Very human labor-intensive; signature file updates sent every 10 minutes or so
- Heuristic technology looks for variety of spam email characteristics, thus it can identify "first time" or altered spam
 - Heuristic technology is better equipped to identify and manage new types of spam attacks



Le moteur heuristique amélioré

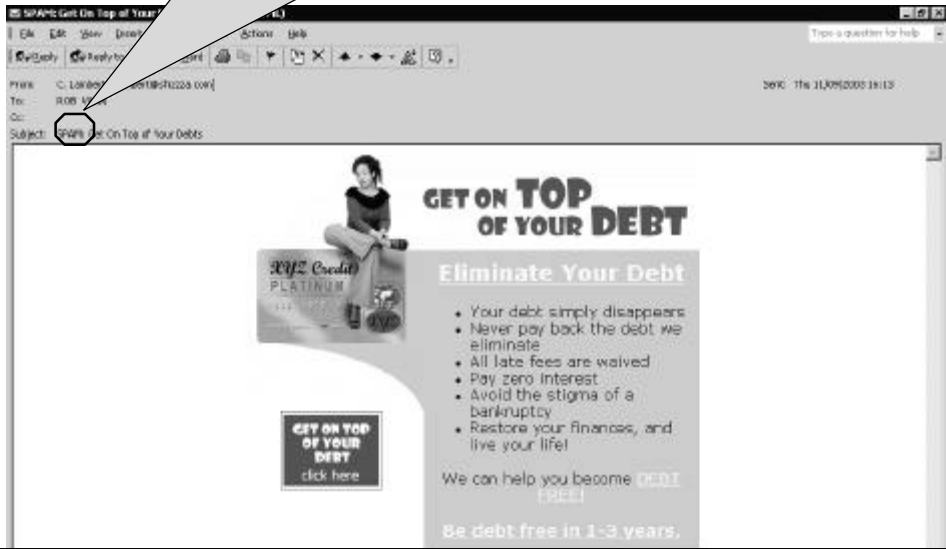
- Le message est évalué comme un TOUT
- PAS seulement évalué par rapport aux mots-phrases
 - Black-listed and White-listed addresses
 - Détecte si passage par plusieurs serveurs
 - Adresses IP falsifiées (Spoofed IP addresses)
 - Good and bad words and phrases (some are +, some are -)
 - Patterns in the body, e.g. short text but several images
 - Short headers (like "Re: hi")
 - URLs with IP addresses instead of domain names, often pointing to image files

Chaque test attribue de mauvais ou de bons points pour arriver à un score final.

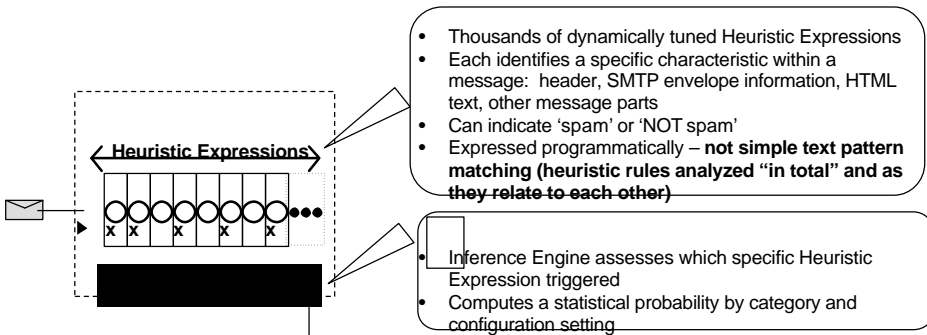


Spam dans l'objet

SPAM inserted into subject line of the message.



Heuristic Scan Engine Process



Peut être rapidement adapté (new categories or methods)

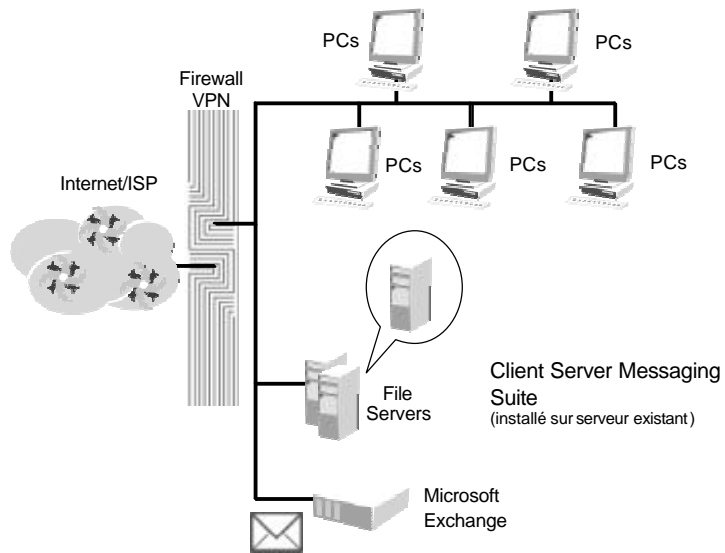
Based on daily analysis of millions of real-world emails

Sample Result

- 98% probability "spam"
 - 99.3% pornographic
- 0.1% probability "NOT spam"



SMB - Windows PCs, File servers, and Microsoft™ Exchange™



PME - Client Server Messaging Suite for PME - Benefits

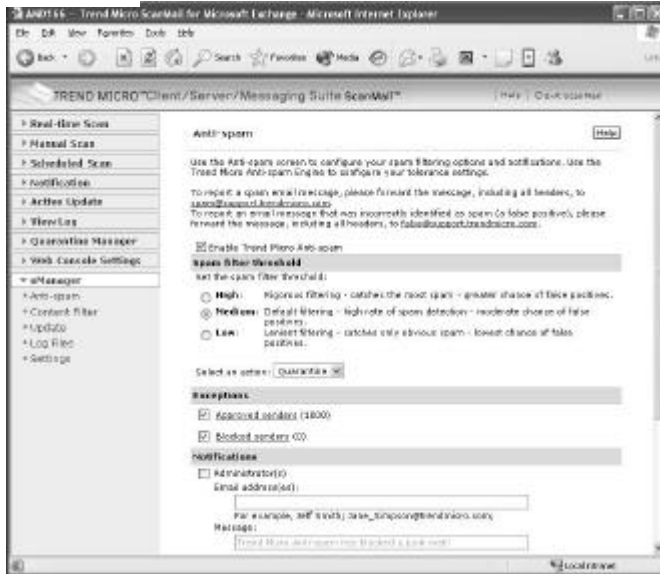
Integrated antispam & content filtering Technology

- Heuristic antispam engine -No editing of spam keyword list
- Réduit le risque des *malicious attacks* en filtrant unwanted emails and unsafe email attachments
- Augmente l'efficacité de l'usage de l'email en bloquant le spam avant qu'il n'arrive dans les mailboxes des utilisateurs
- Meilleur rapport performances/prix que les solutions stand-alone ou services externes



ScreenShot

Facilité d'utilisation!

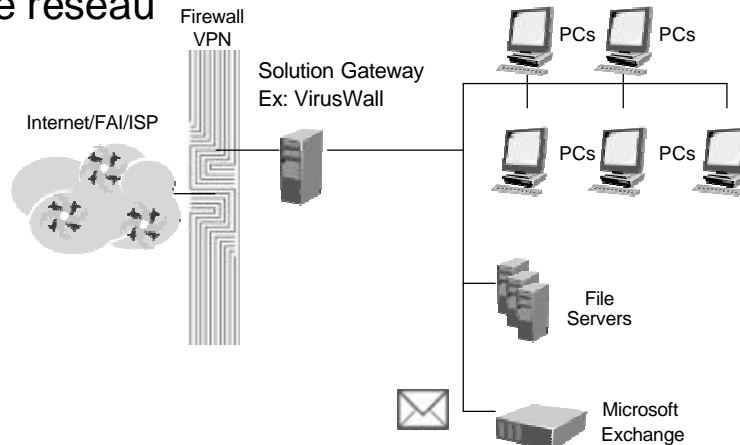


- Actions:
- Quarantine
 - Archive
 - Delete



Shielding internal network from Internet threats...

Stop virus & spam avant qu'ils entrent dans votre réseau





Bénéfices de cette solution

Comprehensive Protection

- All-in-one integrated solution running from one server
 - Email filtering – SMTP & POP3
 - Web filtering – HTTP
 - File download filtering – FTP
- Multi-layer antispam technologies delivers high detection w/low false positives
 - Heuristic engine, signature database, and black & white listings

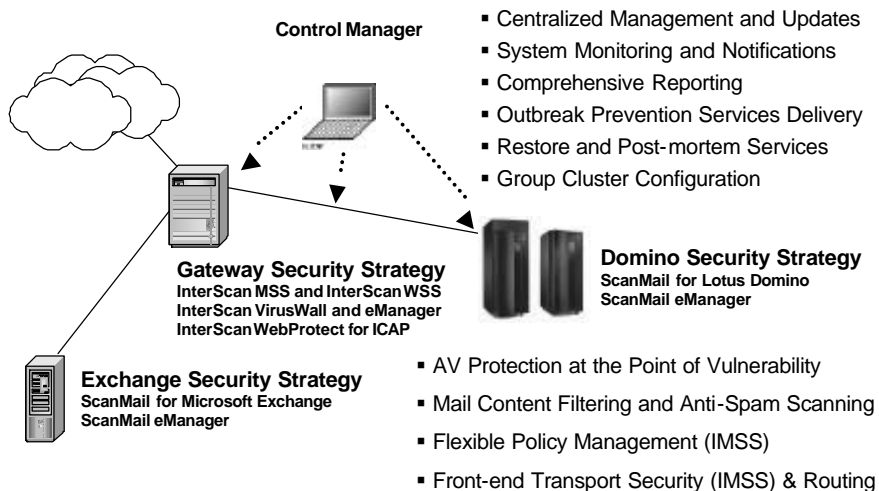
Effortless to deploy & maintain

- Installation wizard
- Single product design
- Single policy ensures consistent protection across company – set and forget.
Stop viruses and spam at the gateway!

“85% of virus, worm, and Trojan comes from the Internet”

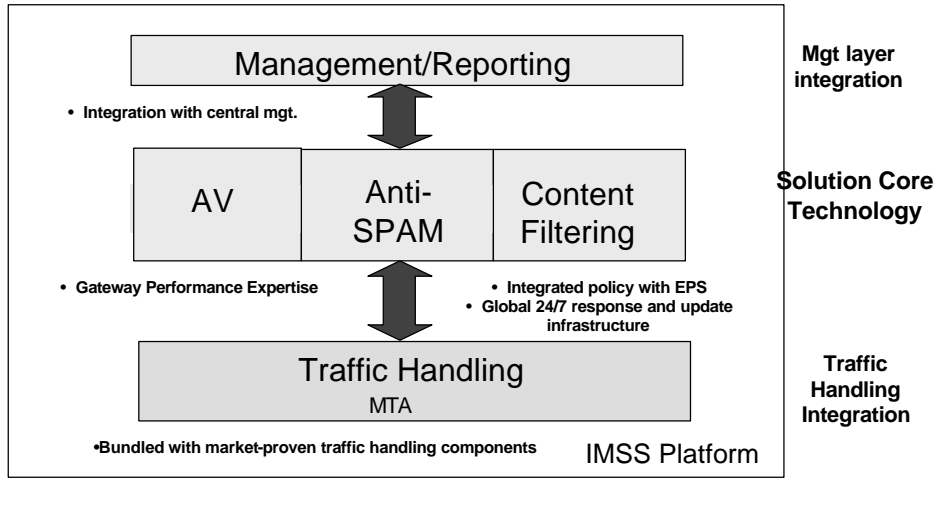


Solution Enterprise Messaging Security





World-class Messaging Platform – IMSS5.5 SPS 2.0 (antivirus, antispam, content filtering)



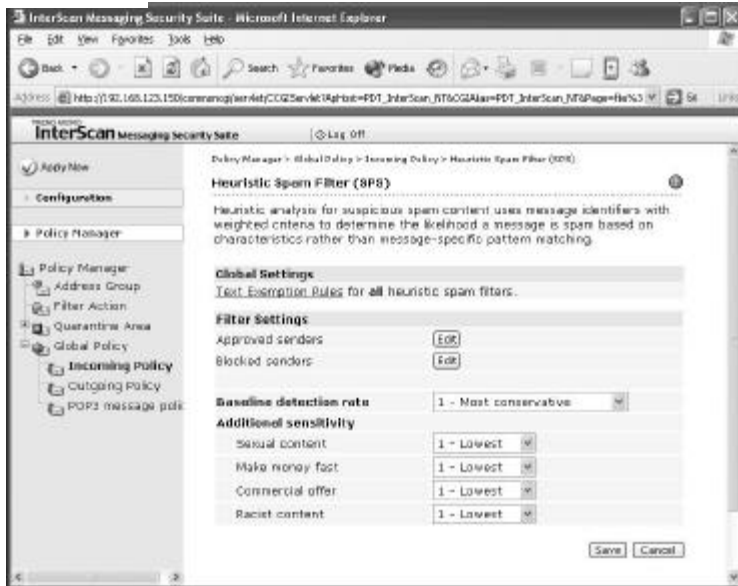
World-class Messaging Platform – IMSS5.5 SPS 2.0 (antivirus, antispam, content filtering)

The screenshot shows the "Filter List" in the InterScan Messaging Security Suite. The table below represents the data visible in the interface:

Index	Filter Name	Origin	Filter Type	Prior Availability and Status	Prior Action	All
1	WU3	Global Policy	Spam Filter	Active	Low	1/0
2	Heuristic Spam Filter (SPS)	Global Policy	Spam Filter	Active	High	1/0
3	SPS5 SGTSP50	Global Policy	Spam Filter	Inactive	High	1/0
4	Profanity	Global Policy	Advanced Content Filter	Inactive	High	1/0
5	Facial Discrimination	Global Policy	Advanced Content Filter	Inactive	High	1/0
6	Spam Detection	Global Policy	Advanced Content Filter	Inactive	High	1/0
7	Housers	Global Policy	Advanced Content Filter	Active	High	1/0



World-class Messaging Platform – IMSS5.5 SPS 2.0 (antivirus, antispam, content filtering)



Les nouvelles techniques des spammers

- **Phishing**

Aux Etats-Unis, le *phishing* aurait déjà fait pas mal de dégâts. Selon le cabinet d'études Gartner, près de 30 millions d'internautes américains auraient reçus des mails frauduleux. Onze millions d'utilisateurs auraient cliqué sur ces courriers et 3 % d'entre eux auraient révélé leurs données personnelles. Gartner estime que les pertes liées au *phishing* ont déjà coûté près de 1,2 milliard de dollars aux banques et aux émetteurs de cartes de crédit.

- **Wi-Fi**

- **GSM ...**



De petits outils très utiles

- *SpamBayes* : plug-in anti-spam pour Microsoft Outlook 2000/XP sous Windows, mais aussi pour Linux et Mac OS. (anglais)
<http://spambayes.sourceforge.net/>
- *SpamPal* : logiciel anti-spam gratuit et en français pour filtrer les spams à partir des black-lists (nombreux plug-ins dont un bayésien). <http://www.spampal.fr>



De petits outils très utiles

- *Traceur VisualRoute* : localise et identifie un serveur, une station de travail ou un site web (tapez son adresse IP ou son URL, puis "Entrée").
<http://visualroute.visualware.com/>
- *HoaxKiller* : Antihoax gratuit en ligne analyse le texte d'un message suspect pour déterminer s'il ne s'agit pas d'un hoax (rumeur ou canular du web), ainsi que certains virus ou tentatives d'escroquerie. <http://www.hoaxkiller.fr/>
- <http://office.microsoft.com/fr-fr/officeupdate/default.aspx>



Panorama de quelques offres du marché (1/2)

Editeur	Nom	Techniques de Filtrage	Architecture	Prix
Alladin	eSafe Gateway	Listes noires. Mises à jour tous les jours. Filtre avec 17 mécanismes différents.	Passerelle. Nécessite serveur dédié.	3168 € pour 50 users et 1 an de maintenance.
Critical Path	Critical Path	Antispam de Brightmail (Symantec)	Solution hébergée	A partir de 0.35 ht par user et par mois si + de 1000 users
Goto Software	Vade Retro	Règles heuristiques, analyse sémantique, signatures HTML	Pour serveurs e-mail. Windows, Linux, et Solaris.	290 € ht pour 25 users et 1 an de MàJ
IPswitch	Imlail Server	Filtrage par listes noires de domaines et d'URL. + de 20 filtres dont un Bayésien, un système d'interrogation DNS inversé et filtres SMTP	Serveur e-mail	730 ht pour Imlail Small Business (5 domaines et 10 mailing lists, users illimités. 1.570 ht pour Imlail Pro (illimité)
IronPort	Serie C	Antispam de Brightmail (Symantec)	Passerelle. Solution hard & soft	10.000 ht pour le C10 (250 users) 25 à 30.000 ht pour le C30 et 55.000 ht pour le C60



Panorama de quelques offres du marché (2/2)

Editeur	Nom	Techniques de Filtrage	Architecture	Prix
Panda	Platinum Internet Security	Listes blanches. Filtres heuristiques.	Soft pour poste client Windows	34 ht ou 68 Ht avec 1 an de services
Symantec	Norton antispam	Possibilité de filtrer les mails en fonction de la langue. Filtre bayésien. Récupération du carnet d'adresses d'Outlook pour la liste blanche.	Soft pour poste client Windows	40 ht par poste
Symantec	Brightmail	Signatures, filtre sur les entêtes, filtre heuristique, listes noires.	Passerelle soft	41 ht par an et par poste (50 à 99 p.)
Trend Micro	Spam Prevention Solution	Filtre heuristique proactif et cumul de différentes techniques. Disponibles aussi en solution PME.	Passerelle soft	23 ht par poste (51 à 100 postes)
CipherTrust	IronMail	Techniques simultanées: filtres bayésiens, filtres d'URL, listes noires et blanches	Passerelle. Solution hard, soft et service	A partir de 9.990 ht pour 100 users
Webwasher	Webwasher Anti Spam	Listes blanches et noires, filtres bayésiens, analyse texte et entêtes	Passerelle soft	24 ht par user (50 postes)
Roaring Penguin	Canit	Listes noires et blanches	Unix, Linux avec SendMail. Code source fourni.	6 ht par an et par boîte mail la 1 ^{ère} année.
Spam Assassin	Spam Assassin	Listes noires, filtres bayésiens, analyse du texte et des entêtes	Passerelle soft	Open Source Gratis



L'avenir ? L'authentification des e-mails

On ne changerait pas SMTP, mais on y apporterait des *plug-in* afin de responsabiliser l'auteur d'un e-mail

- 1 Authentification de l'adresse IP (ou du chemin) : *Caller ID de Microsoft (valide l'entête From: de l'utilisateur valide parmi d'autres entêtes) et SPF de Meng Wong (valide l'adresse SMTP Mail From: non affichée)*
- 2 Cryptographie à base de clé publique et clé privée: *DomainKeys de Yahoo! Adapté au e-commerce. Signature aux messages envoyés et valide l'entête From: user visible*



L'avenir ? L'authentification des e-mails

Sender ID de Sendmail, c'est un peu la fusion de Caller ID et de SPF

1. Expéditeurs publient les IP de leurs serveurs mail sortants dans le DNS.
2. Le système mail recevant les courriers examine chaque message pour déterminer le domaine prétendu responsable ou l'adresse Internet qui prétend avoir envoyé le message.
3. Les serveurs mail recevant les messages (entrants) effectuent une requête DNS pour obtenir la liste des adresses IP des serveurs mails sortants du domaine prétendu responsable. Ensuite, vérification si adresse IP est bien sur la liste. Si ce n'est pas le cas, il est probable que le message a été 'spoofé' (usurpé) !

... mais il est probable que plusieurs mécaniques coexisteront à base de challenge-response.



L'avenir ?

- *Serveurs Mares de goudron*. Si même utilisateurs envoient alors 5 sec entre messages
- *Listes grises*. Retarder tout message pour lequel l'IP n'est pas connue
- Faire payer comme un timbre. Micropaiement.
- Paiement en temps de calcul du PC émetteur. *Penny Black par Microsoft*. (temps de calcul de +/- 10 sec)



Risques - PC, serveurs et MS Exchange



- Votre serveur de messagerie Exchange peut devenir un nid de virus (pièces jointes, ...)
- Le spam et les envois de messages en masse effectués par les virus diminuent la productivité
- Les e-mails infectés sont transmis aux clients et aux partenaires
- Le contenu répréhensible des e-mails peut vous mettre en porte-à-faux vis-à-vis de la loi (black-list, spam-relay, ...)



Risques - Passerelle Internet



85 % des infections virales sont transmises par Internet

Les logiciels antivirus des postes de travail et de la messagerie ne sécurisent pas toujours la navigation sur le Web, le courrier Internet (HTTP) et les téléchargements (FTP).

Le spam diminue les performances et la productivité de tout le réseau



de Tésor® Computers optez pour la sécurité

Rue du Centre, 57 • B-4800 Verwiltz • BELGIUM • Tel. +32 (0)87 233 770 • Fax. +32 (0)87 233 509 • mail : info@tesor.be
Nouvelle Adresse d'Orléans • Population: 1 • 01010 Orgeron • BELGIUM • Tel. +32 (0)2 700 423 3 • Fax. +32 (0)2 700 42 42

Questions ?



de Tésor® Computers optez pour la sécurité

Rue de Centre, 57 • D-4800 Verviers • BELGIUM • Tel. +32 (0)87 293 770 • Fax. +32 (0)87 293 509 • mail : info@detesorbis.be
Nouvelle Adresse : 100 Louvain • Organisme : S • D-1039 Olegem • BELGIUM • Tel. +32 (0)2 709 091 3 • Fax. +32 (0)2 709 09 20

Je vous remercie pour votre attention.

Jean-Paul Rosette
de Tésor SA
Networking & Security