
Comment garder le spam à l'écart de votre réseau

A quelles fonctionnalités faire attention dans la technologie anti-spam

Un guide pour les acheteurs de logiciels anti-spam, ce livre blanc met en relief et explique les fonctionnalités importantes d'un logiciel anti-spam.

Introduction

Ce livre blanc vous aide à identifier les fonctionnalités clés nécessaires pour combattre efficacement le spam.

| | |
|--|---|
| Introduction..... | 2 |
| La croissance et le coût du spam..... | 2 |
| Choisir le bon logiciel anti-spam..... | 2 |
| Comment GFI MailEssentials s'attaque au spam | 6 |
| A propos de GFI Software..... | 8 |

La croissance et le coût du spam

Le groupe Radicati, une société de recherche américaine, estime que 52% du trafic mondial des emails actuel est constitué de messages spam et prédit que ce taux atteindra 70% d'ici 2007. De même, l'Union Européenne estime que 50% de tous les emails sont des messages spam.

Cela signifie que les employés doivent consacrer une partie de leur temps de travail à traiter le spam, d'où une diminution de productivité (et une augmentation de la frustration!). La perte de productivité est le coût principal engendré par le spam, en particulier lorsque autant de messages indésirables sont reçus chaque jour. A cela s'ajoute le gaspillage de bande passante ainsi que d'autres dépenses de stockage et d'infrastructure de réseau. De plus, en supprimant massivement le spam on encourt également le risque de supprimer un message important.

Ferris Research a compté que si un employé recevait seulement 5 messages spam par jour, et passait 30 secondes sur chaque, il perdrait 15 heures par an à trier son courrier indésirable – multipliez ce chiffre par le salaire à l'heure de chaque employé dans votre compagnie et vous aurez une idée du coût de revient du spam à votre entreprise. Le groupe Radicati Group a rapporté que le spam a coûté aux Technologies Informatiques environ \$49 par boîte aux lettres en 2003, et s'attend à ce que ce chiffre atteigne \$257 par boîte aux lettres en 2007.

Il est essentiel de mettre fin au spam pour économiser du temps, de l'argent de la bande passante. Une autre façon de faire avancer les choses serait de conseiller aux utilisateurs du réseau de garder leur adresse email privée (ne pas l'envoyer à des forums de messages etc.). Cependant, sans parler du bon sens, vous avez aussi besoin de déployer un utilitaire anti-spam de serveur efficace.

Choisir le bon logiciel anti-spam

Sur le marché, beaucoup de logiciels sont à votre disposition pour vous aider à combattre le spam ; mais tous ne sont pas assez avancés pour combattre le spam. Ci-dessous, vous

trouverez un nombre de fonctionnalités/problèmes clés qui sont très importants.

Logiciel serveur ou client ?

Lutter contre le spam au niveau du client nécessite beaucoup plus de temps qu'au niveau du serveur. Cela exige que vous déployiez le logiciel anti-spam sur chaque poste de travail de votre réseau et implique la mise à jour fréquente des règles anti-spam sur chacun d'entre eux. Cela signifie aussi que votre système de messagerie est débordé de messages inutiles attendant d'être effacés. Qui plus est, un logiciel client implique aussi que vos utilisateurs passent du temps à identifier le spam ou à mettre à jour leurs jeux de règle: et c'est cela même que vous cherchez à éviter en combattant le spam !

De plus, il ne possède pas les informations et les ressources du logiciel anti-spam de serveur – il ne vous permet pas de contrôler les serveurs expéditeurs, par exemple. Pour bloquer le spam de manière efficace, vous devez avoir un produit anti-spam basé sur le serveur car ils offrent les avantages suivants :

1. L'installation sur la passerelle évite le déploiement individuel et réduit le casse-tête administratif impliqué par les solutions clientes.
2. Bien meilleur marché.
3. Empêche le spam de pénétrer dans votre infrastructure de messagerie, ainsi celle-ci n'est pas saturée de messages indésirables.
4. Le logiciel anti-spam de serveur possède davantage d'informations et peut détecter plus efficacement le spam.

Technologie de filtrage Bayésien

Il y a quelques années, la plupart des produits anti-spam employaient simplement une liste de mots-clés pour identifier le spam. Un bon jeu de mots-clés limite en effet considérablement le spam. Cependant, de nos jours, le blocage de spam basé sur un jeu de mot clé génère trop de faux positifs et requiert trop de mises à jour manuelles.

Il est maintenant grandement reconnu par les experts et les rapports que la meilleure façon de bloquer le spam est de se servir d'un filtre Bayésien. Un filtre Bayésien utilise une approche mathématique basée sur le spam connu et le ham (email légitime). Cela lui donne un énorme avantage sur les technologies spam obsolètes qui ne font que vérifier les mots clés ou s'en remettent au téléchargement des signatures de spam connues. Plus d'informations sur le filtrage Bayésien se trouvent dans le livre blanc intitulé Pourquoi le filtre Bayésien est la technologie la plus efficace à l'adresse suivante : <http://www.gfsfrance.com/fr/whitepapers/why-bayesian-filtering.pdf>.

En bref, les avantages du filtre Bayésien sont :

1. Prend en compte le message dans son intégralité, non seulement les mots clés ou les

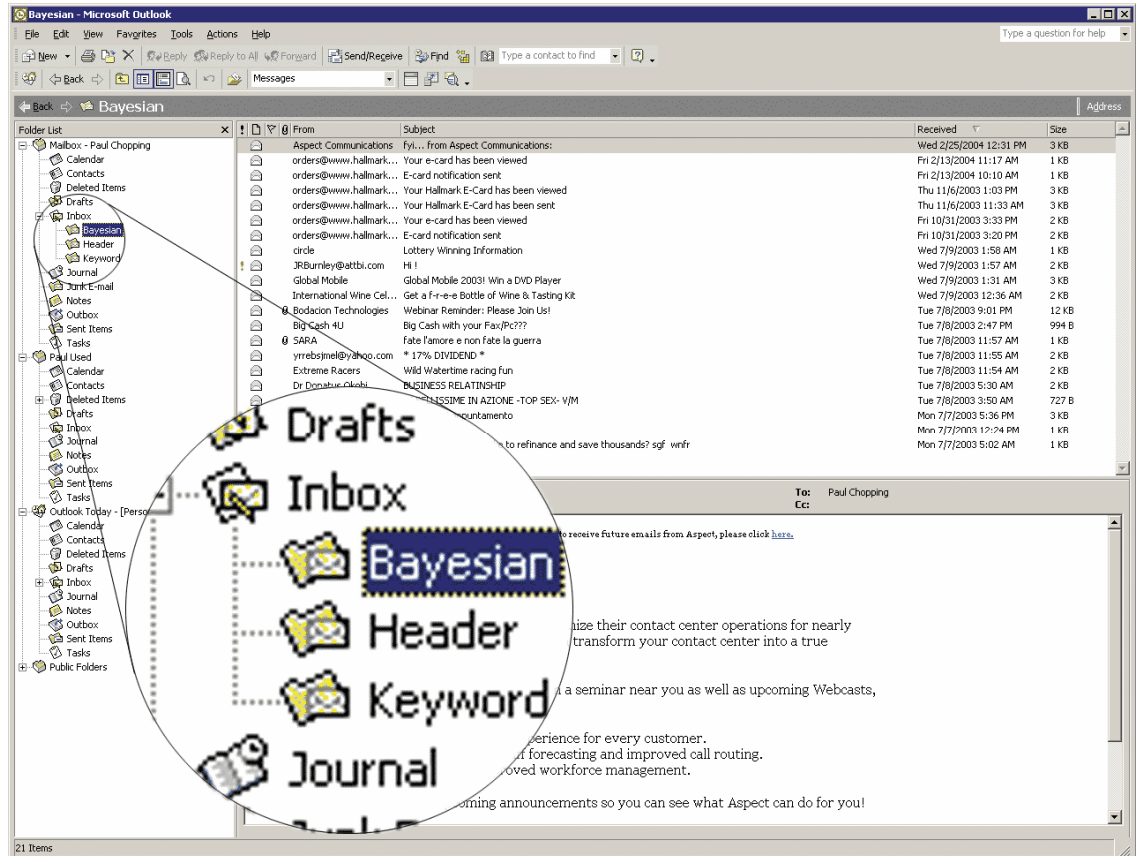
signatures spam connues

2. Apprend à partir du courrier d'envoi (ham) et réduit grandement par là les faux positifs
3. S'adapte avec le temps par un apprentissage des nouvelles formes de spam et de courrier valide
4. L'ensemble de données est unique pour chaque société, et est ainsi impossible à éviter
5. Multilingue et international.

Fichier de données sur mesure pour le filtre Bayésien

Il est essentiel que le filtre Bayésien utilise un jeu de données qui a été personnalisé selon votre entreprise : les données ham DOIVENT provenir de votre boîte d'envoi (de cette façon, une période d'apprentissage initiale rend le filtre Bayésien unique à votre compagnie). Des logiciels anti-spam utilisent un fichier de données ham général qui est fourni avec le produit. Un exemple de filtre spam est le filtre d'Outlook ou Exchange Server Internet Message Filter. Bien que cette technologie ne requière pas de période d'apprentissage initiale, elle a deux défauts majeurs :

1. Le fichier de données ham est ouvertement disponible et peut donc être piraté par des spammers professionnels et donc être contourné. Si le fichier de données ham est spécifique à votre compagnie, il est donc inutile de le pirater. Par exemple, il y a des hacks disponibles pour contourner le filtre anti-spam Microsoft Outlook 2003.
2. Ensuite, le fichier de données ham est général, et n'est pas créé sur mesure aux besoins de votre compagnie, il ne pourra pas être aussi efficace qu'un produit personnalisé. Vous aurez beaucoup plus de faux positifs. Par exemple, une institution financière qui utilise le terme « hypothèque » assez souvent obtiendrait beaucoup plus de faux positifs avec un fichier ham général.



Passer en revue le spam, est chose facile s'il est enregistré dans un sous dossier de la boîte de réception de l'utilisateur

Mise à jour automatique du fichier de données spam pour le filtre Bayésien

Le fichier de données spam du filtre Bayésien doit être constamment mis à jour avec le plus récent logiciel anti-spam. Ceci permet au filtre Bayésien de connaître les derniers tours des spam, et d'offrir un taux plus élevé de détection contre le spam (remarque : cela est possible une fois la période d'apprentissage de deux semaines terminée). Choisissez un produit anti-spam qui se chargera de récupérer les données spam à votre place et qui vous permettra de télécharger ces mises à jour automatiquement !

Bien savoir manier le spam pour le passer en revue efficacement

Les faux positifs vont de pair avec les technologies anti-spam, par exemple, un message peut être balisé en tant que spam bien qu'il ne s'agisse pas réellement d'un message spam. Un bon logiciel anti-spam devrait donc fournir un moyen simple et facile de passer en revue le courrier balisé comme spam rapidement et efficacement.

De façon à ce que les administrateurs ne perdent pas leur temps et n'aient pas de problèmes

avec le spam, le logiciel anti-spam doit inclure une option qui redirige le courrier identifié comme spam directement vers un dossier de courrier indésirable. De plus, le logiciel devrait trier le spam vers des dossiers différents en fonction de ce qui a permis son identification. L'accès rapide aux messages balisés comme spam est une aide précieuse pour que l'utilisateur puisse les passer en revue efficacement. Certains produits anti-spam demandent que l'utilisateur se connecte à un système basé sur le Web et revoie ses messages les uns après les autres – en pratique, cela est une tâche énorme pour l'utilisateur et l'amènera à ne pas se servir de cette fonction très souvent.

Listes blanches flexibles pour réduction des faux positifs

Le logiciel anti-spam doit avoir un moyen efficace de construire des Listes blanches étendues. Elles doivent identifier tous les partenaires commerciaux légitimes, de façon à ce que leurs messages ne soient pas marqués comme spam. Un bon anti-spam doit pouvoir créer et mettre à jour ces listes blanches automatiquement.

Comment GFI MailEssentials s'attaque au spam

L'approche de GFI MailEssentials à la détection du spam est basée sur les méthodes et les technologies suivantes :

1. **Attaque le spam au niveau du serveur** - GFI MailEssentials s'installe sur votre serveur Exchange 2000, ou avant votre serveur de messagerie (si vous utilisez Exchange 5.5 ou un autre serveur de messagerie). Il détecte le spam AVANT qu'il n'atteigne votre serveur de courrier. Ainsi, le spam ne sature pas votre système de messagerie et les mises à jour de règle de détection du spam doivent uniquement être déployées sur la machine de GFI MailEssentials. Les listes blanches (domaines/email, dont vous souhaitez toujours recevoir le courrier) et des listes noires (domaines/email dont vous ne voulez pas recevoir le courrier) peuvent être utilisés au niveau du serveur.
2. Analyse le contenu des emails en utilisant **un filtre de Bayes** et utilise les données ham spécifiques à votre compagnie. Celles-ci sont automatiquement mises à jour en téléchargeant les dernières données à partir du site de GFI Software. Pour plus d'informations sur les filtres Bayésiens, veuillez consulter le livre blanc sur <http://www.gfsfrance.com/fr/whitepapers/why-bayesian-filtering.pdf>.
3. **Réduction des faux positifs grâce à la liste blanche automatique** - GFI MailEssentials comprend un outil de gestion de liste blanche breveté en suspend. Cette technologie, unique en son genre, fait que tous les partenaires commerciaux sont ajoutés automatiquement à votre liste blanche – sans besoin d'administration – et leurs messages ne passeront pas par le filtre anti-spam, réduisant grandement les faux positifs.
4. **Gestion flexible du spam** – Après avoir reconnu un message comme spam, il peut le transférer vers un sous dossier de la boîte de réception de l'utilisateur. Si celui-ci décide

qu'il s'agit d'un message légitime (par exemple une lettre de nouvelles qu'il désire recevoir), l'utilisateur peut ajouter l'expéditeur à la liste blanche.

5. GFI MailEssentials a une option de **vérification par mot clé** pour que les administrateurs puissent parfaire leur réglage des filtres anti-spam.
6. Pour une plus grande protection, le filtrage Bayésien est renforcé par un certain nombre de **technologies de détection anti-spam**, dont une analyse intelligente des en-têtes de courrier et une comparaison des expéditeurs avec les listes noires et les listes noires publiques telles que ORDB ou SpamHaus.

A propos de GFI Software

GFI est l'un des leaders dans le domaine de la réalisation de logiciels qui fournit une seule source intégrée permettant aux administrateurs de résoudre les problèmes de sécurisation de réseaux, de contenu et de messageries. Grâce à sa technologie innovatrice, une stratégie agressive de commercialisation et sa concentration sur le marché de petites et moyennes entreprises, GFI répond aux besoins de continuité d'affaires et de productivité des entreprises et d'autres organisations sur une grande échelle. Fondée en 1992, GFI est une entreprise internationale qui possède des bureaux à Malte, à Londres, Raleigh, Hong Kong, Adelaïde et à Hambourg avec plus de 200.000 installations de ses logiciels à travers le monde. GFI est une entreprise spécialisée et possède un réseau de plus de 10.000 partenaires à travers le monde. Partenaire stratégique de Microsoft, GFI est membre certifié du partenariat Microsoft Gold Certified Partner. Pour plus d'informations à propos de GFI, visitez le site <http://www.gfsfrance.com>.

© 2007 GFI Software. Tous droits réservés. L'information contenue dans ce document représente le point de vue actuel de GFI sur les questions abordées à la date de sa publication. Etant donné que GFI doit répondre aux conditions dynamiques du marché, il ne devrait pas être interprété comme un engagement de la part de GFI, et GFI ne peut pas garantir l'exactitude d'aucune information présentée après la date de la publication. Ce livre blanc est seulement à titre informationnel. GFI NE FAIT AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, DANS CE DOCUMENT. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor et leurs logos de produit sont des marques déposées ou des brevets commerciaux de GFI Software aux Etats-Unis et/ou dans d'autres pays. Tous les noms de produit ou d'entreprises mentionnés ci-dessus peuvent être les marques déposées de leurs propriétaires respectifs.