



**vaderetro**  
Outlook et Outlook Express

# Press book

( Q4 - 2007 )



**GOTO** Software  
DEVELOPPEMENTS DURABLES

caractères, elle est déformée afin que le texte reste lisible uniquement pour l'œil humain. Comme la mode, le spam a ses tendances, les dernières font appel aux fichiers utilisant les formats PDF et XLS (Acrobat et Excel). Ces documents sont le nouveau support des textes et images publicitaires.

### La lutte antispam repose sur l'utilisation de filtres d'analyse

Pour faire face à ces technologies d'intrusion, les logiciels de courrier électronique ont donc fort à faire. Difficile en effet de différencier un courrier légitime d'un spam. Pourtant, au fil des années, les éditeurs ont amélioré les filtres, et les résultats que nous avons obtenus avec des messageries traditionnelles sont plutôt bonnes. Qu'il s'agisse d'Outlook ou de Thunderbird, toutes les versions récentes de ces logiciels possèdent des mécanismes antispams. Ils sont basés sur l'analyse sémantique des e-mails, analyse renforcée, progressivement, par un moteur d'apprentissage. À cette analyse s'ajoute l'appel à une base de données régulièrement alimentée (par Windows Update pour Outlook 2003/2007) et contenant les signalements des spams identifiés.

### Les logiciels spécialisés ne manquent pas d'inventivité

Les programmes de messagerie attaquent donc le spam sur deux fronts : non seulement le contenu, mais aussi l'enveloppe (l'en-tête) des e-mails. L'en-tête est intéressant à plus d'un titre car il rassemble des informations sur la provenance de l'e-mail (adresse IP de l'envoyeur, logiciel utilisé pour l'envoi, adresse de retour...). En listant ces caractéristiques, il devient possible de lutter en temps réel contre le spam. L'ennui,

## 6 solutions passées au crible

Solutions	Goto Software Vade Retro	Kaspersky Internet Security V7.0	McAfee Internet Security suite	Windows <sup>2007</sup> SPAMfighter	Spamihilator	BitDefender Internet Security 2008
Adresse web	www.anti-spam.fr	www.kaspersky.fr	www.mcafee.fr	www.spamfighter.com	www.spamhilarator.com	www.bitdefender.fr
Qualité de filtrage du spam	5/5	1/5	4/5	5/5	3/5	1/5
Connaissances antispams mutualisées	Oui	Non	Oui	Oui	Oui	Oui
Facilité d'utilisation	5/5	3/5	4/5	4/5	1/5	4/5
Nombre de faux positifs	0	9	20	5	20	12
Pourcentage de spam véritable arrêté / spam total	98,5 %	23,5 %	90,2 %	100 %	58,8 %	26 %
Compatibilité	Outlook Express 2000/2003	Indépendant du client de messagerie	Outlook Express 2000/2003, Windows Mail, Thunderbird, Eudora	Outlook Express 2000/2003	Outlook Express, Eudora, Thunderbird, Incremail	Outlook Express 2000/2003/2007, Windows Mail, Thunderbird
Prix	29 € par an	69,95 € par an	69,95 € par an	Gratuit avec publicité ou 25 € par an	Gratuit	22,95 €
Note globale	9/10	4/10	7/10	10/10	4/10	5/10
Remarques	Abonnement à l'année	Liste de critères de filtrage optionnels trop longue, apprentissage obligatoire	Ne filtre pas les fichiers en .pdf	Ajoute une ligne de publicité dans les e-mails si le logiciel n'est pas acheté	Interface trop complexe	Totalement inefficace sans apprentissage

c'est qu'il faut mettre à jour très régulièrement les données du programme. C'est là que certains des logiciels spécialisés dans la chasse au spam prennent le dessus par rapport aux mécanismes d'Outlook et de Thunderbird : Spamihilator, SPAMfighter ou Vade Retro utilisent des serveurs "DNSSB" (DNS Servers Blacklist) et "DCC" (Distributed Check Clearinghouse). Ces derniers recensent, en temps réel, l'ensemble des ordinateurs géné-

rateurs de spams dans le monde pour les premiers, et les signatures numériques des spams pour les seconds. Grâce à des mises à jour très régulières, ces logiciels antispams récupèrent la majorité des courriers indésirables. Le système possède quand même une faille : certaines newsletters, à force d'être signalées par des utilisateurs, se retrouvent classifiées comme du spam... De plus, l'automatisme des

## Tous contre le spam

Au niveau mondial, la lutte contre le spam s'organise : des listes d'adresses IP utilisées par les spameurs sont accessibles aux logiciels de lutte contre le spam. Le même système est en place pour référencer les signatures électroniques des pièces attachées au spam. Tous ces serveurs sont alimentés par les serveurs e-mail des fournisseurs d'accès à internet ou d'hébergeurs avec plus ou moins de réussite ; il n'est pas rare, en effet, que des courriers envoyés d'un FAI à un autre soient arrêtés. Pour autant, la mutualisation des données semble être la seule voie pour contrer la prolifération du spam. En mai dernier, le gouvernement français a décidé de créer une plate-forme de signalement des courriers indésirables, Signal Spam (www.signal-spam.fr/). Ce site – tout ce qu'il y a de plus officiel – propose de télécharger une barre d'outils qui vient s'intégrer dans l'interface des messageries Outlook 2003/2007 et Thunderbird. Cette barre signale chaque courrier indésirable et envoie les données vers cette plate-forme. Ces signalements permettront peut-être à l'Association de repérer les sociétés ou les personnes qui utilisent le spam, et d'entreprendre des actions judiciaires contre elles.



procédures et le partage des ressources font qu'une erreur prend tout de suite de l'ampleur. Ainsi, selon nos constatations, le site Signal Spam ([www.signal-spam.fr](http://www.signal-spam.fr), lire encadré page 58) a été banni par les webmails Gmail et Hotmail... Impossible de recevoir la confirmation d'inscription à ce site de lutte contre le spam lorsque l'adresse d'abonnement se trouve chez ces webmails...

Ce genre d'erreur est à l'origine d'une nouvelle forme de protection : l'authentification de l'expéditeur. Le principe est simple. Au premier e-mail, l'expéditeur doit se rendre sur une page web pour s'identifier (lecture d'un texte déformé, impossible à déchiffrer par un logiciel). L'adresse de l'expéditeur est alors entrée dans la base des courriers valides. Si l'action n'est pas réalisée, le courrier rejoindra un répertoire de confirmation duquel il pourra être récupéré et validé par le propriétaire de la boîte aux lettres.

## Les solutions à mettre en place sont nombreuses

Avant de sortir toute cette artillerie, il existe des solutions intermédiaires. Tout d'abord, en suivant nos conseils (lire encadré page 56), vous éviterez d'intégrer les listes des spammeurs. Ensuite, pour des adresses non utilisées sur le web (forums, newsgroups...), Outlook et Thunderbird suffisent à évacuer le spam traditionnel. Leurs filtres personnalisables sont autant d'armes pour faire barrage aux courriers non désirés.

En revanche, si votre adresse e-mail a déjà rejoint les listings de spammeur, vous trouverez page 58, le tableau des six solutions que nous avons testées. Les logiciels ont été soumis à un test complet : nous avons créé une boîte aux lettres et diffusé son adresse sur de nombreux sites et newsgroups. Cette adresse reçoit aujourd'hui près d'une centaine de spams par jour. Nous avons recueilli 318 courriers, contenant 41 messages légitimes et 277 spams, puis nous avons comparé

les tris effectués par les différentes solutions. Pour tester plus en profondeur les mécanismes de protection, nous avons même simulé l'émission d'un e-mail par un serveur de courriers installé sur notre PC, puis nous avons envoyé un véritable spam depuis cette machine (un fichier au format PDF) afin de constater comment les filtres allaient se comporter. Enfin, nous avons aussi évalué l'ergonomie de l'interface en tenant compte du temps passé par l'utilisateur pour mettre en place le paramétrage.

## Des résultats mitigés selon les méthodes utilisées

Les résultats sont en demi-teinte : les logiciels utilisant uniquement des filtres sur les contenus avec un apprentissage ont été maltraités par notre test qui ne prévoyait aucun temps d'adaptation. Nous avons estimé qu'un filtre, même sans apprentissage, devait être un minimum efficace... ce qui n'est pas le cas pour McAfee, BitDefender Internet Security et Kaspersky. Ces deux derniers se partagent la palme de l'inefficacité avec, respectivement, 246 et 242 e-mails considérés



**Performance** Le logiciel Vade Retro fait des miracles : sur 277 spams, seuls trois messages indésirables ont traversé ses filtres.

comme légitimes (notre boîte n'en comptait que 41 !). Ces trois logiciels ont laissé passer massivement le spam par fichier au format PDF. Pour continuer avec les mauvais élèves, Spamihilator nous est apparu comme le programme le moins pratique avec une interface séparée du logiciel qui récupère les e-mails. Difficile de s'y retrouver : les courriers légitimes arrivent dans la boîte aux lettres, les suspects restent en quarantaine pour

## 7 étapes pour paramétrer l'antispam SPAMfighter



**1 Mise à jour de la blacklist** SPAMfighter est apparu lors de nos tests comme l'une des solutions les plus performantes. Cependant, pour délivrer toute sa puissance, encore faut-il apprendre à maîtriser toutes ses fonctionnalités. La première étape consiste à mettre à jour la blacklist, ou liste d'émetteurs reconnus de spams. Dès son installation, SPAMfighter va récupérer une liste à jour des derniers spams. Pour cela il faut que votre pare-feu laisse passer la communication avec le serveur. Si ce n'est pas le cas, réglez votre firewall : la mise à jour très régulière du logiciel est indispensable à son efficacité.

### Special internet pricing!

Viagra \$1.79  
 Cialis \$2.69  
 Valium \$2.48  
 Ambien \$3.14  
 Levitra \$3.96  
 Zoloft \$3.30  
 Phentermine \$5.00  
 Viagra Soft Tabs \$2.05  
 Cialis Soft Tabs \$3.93

More than 100 popular products available  
 We ship Worldwide directly to your home  
 No Doctor visit/prescription is not required

**Subterfuge** Avec un texte dans une image et du texte réel tiré au hasard de pages internet, les logiciels antispams ont fort à faire.

l'apprentissage, et les spams reconnus sont dirigés vers la corbeille... S'ils s'avèrent légitimes, vous devrez les restaurer et relancer la récupération des e-mails dans votre logiciel de courrier. Terminons par les meilleurs : les deux logiciels qui nous ont donné satisfaction sont Vade Retro et SPAMfighter. Sans aucun entraînement ni paramétrage fastidieux, tout deux ont arrêté la quasi-totalité des spams. Vade Retro a laissé passer seulement trois e-mails non désirés (des fichiers au format PDF dont la signature ne devait pas être intégrée dans la base de données du logiciel) et surtout il n'a bloqué aucun courrier légitime. Mieux, il a réussi à repérer notre spam et a bien catalogué les e-mails suivants en provenance de notre serveur. Son concurrent gratuit a presque fait aussi bien avec aucun spam dans la boîte aux lettres et cinq courriers légitimes bloqués. Seul petit regret, cette version gratuite de SPAMfighter ajoute une ligne de publicité à la fin de chaque e-mail envoyé. Ce sont donc ces deux solutions que nous vous conseillons si votre boîte regorge d'e-mails non sollicités.

Jean-Philippe Bay

## Créez et gérez une adresse e-mail temporaire

Pour bien choisir son adresse temporaire, il faut tout d'abord trouver un hébergeur qui utilise un système antispam. Gmail, Live Mail et Yahoo! Mail sont de bons candidats. Ensuite, il faut pouvoir le consulter avec son client de messagerie. Gmail et Yahoo! Mail proposent un service POP compatible avec tous les logiciels de courrier électronique. Enfin, une adresse temporaire étant destinée à recevoir de très nombreux courriers non désirés, il faut disposer de suffisamment d'espace... Yahoo! Mail (mail.yahoo.fr) propose une capacité de stockage illimitée et une bonne gestion des courriers indésirables (vidage du répertoire spam traité jours après réception). Il constitue, actuellement, le meilleur choix pour une adresse temporaire. Une fois l'adresse créée, il faut activer le support du service POP pour y accéder par le biais d'un logiciel de messagerie. Par exemple, dans la fenêtre de Yahoo! Mail, cliquez sur le bouton **Options** en haut à droite.



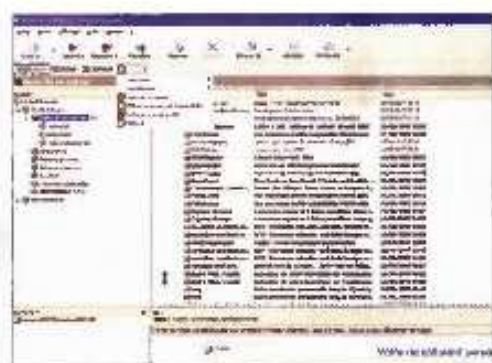
puis rendez-vous sur **Options de mail** ; là vous trouverez l'onglet **Transfert et Accès POP**. Cette page vous donne la possibilité de choisir de télécharger, ou pas, les courriers considérés comme du spam, voire d'y ajouter un en-tête (spam) facilement gérable par votre client e-mail.



**2 Créez un compte** Vous pouvez ainsi gérer votre abonnement. Avec cette option, il est possible de récupérer les contacts que vous avez entrés dans la Liste Blanche du soft, et donc réinstaller SPAMfighter sur votre PC sans perdre cette liste.



**3 Bloquez et débloquez** Une fois votre messagerie lancée, SPAMfighter trie le courrier. Si un spam est passé, sélectionnez-le et cliquez sur **Bloquer**. Inversement (pour un courrier légitime classé en spam), sélectionnez-le et cliquez sur **Débloquer**.



**4 Gérez vos répertoires** Pour effacer tout le dossier spam, cliquez sur **Plus... > Effacer le contenu du dossier spam**. Si votre BAL (ou un répertoire) contenait déjà des spams, sélectionnez le dossier, cliquez sur **Plus... > Nettoyez un dossier**.



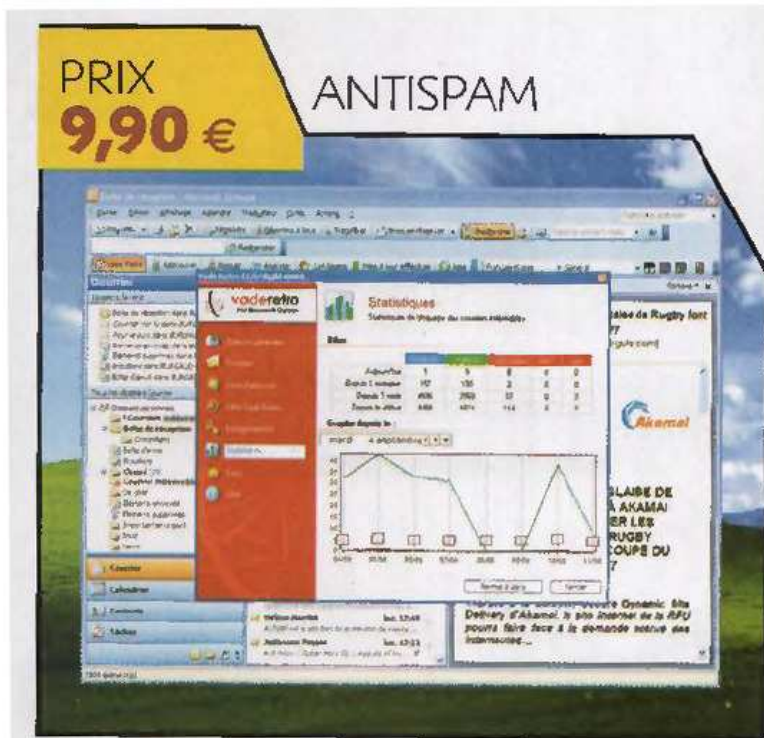
**5 Listes Blanches/Noires** SPAMfighter peut gérer des adresses autorisées ou bloquées : cliquez sur **Plus... > Options > Paramètres du filtre > Listes Blanches / Listes Noires**. Les boutons **Ouvrir** répertorient les adresses des différentes listes.



**6 Paramétrez le filtrage** Pour moduler la sévérité du filtrage, cliquez sur **Plus... > Options**. Vous avez le choix entre cinq niveaux de filtrage. Le plus élevé bloque toutes les adresses qui ne sont pas déclarées dans votre Liste Blanche.



**7 Mettez à jour votre logiciel** Outre les mises à jour de son filtre, le logiciel peut être également updaté. Dans les options du logiciel, cliquez sur le lien **Aide**, puis sur **Mise à jour**. Vous pouvez aussi choisir une mise à jour automatique du programme.



## GOTO VADE RETRO

Débarrassez-vous des messages indésirables.

Les messages électroniques indésirables sont le mal du siècle. Selon les estimations les plus sombres, 85 % des messages échangés seraient du spam. Si votre boîte de réception est touchée, il vous faut un outil antispam : *Vade Retro* est une solution par abonnement compatible avec *Outlook*, *Outlook Express* et *Windows Mail*. Goto Software propose trois formules : 990 euros pour 3 mois, 1750 euros pour 6 mois et 2990 euros pour un an de mise à jour du filtre. *Vade Retro* analyse votre boîte

pour y dénicher les spams déjà reçus et trie aussi les messages dès réception. Ceux détectés comme indésirables sont déplacés dans un dossier dédié et c'est à vous de décider ensuite de les conserver ou de les détruire. À peine installé, le filtre se révèle performant : il se trompe rarement et laisse passer peu de spam. Pendant toute la durée de votre abonnement, il est mis à jour pour suivre les évolutions des techniques utilisées par les spammers et continuer à vous en protéger de la façon la plus efficace possible.

■ Moyennant un abonnement, *Vade Retro* vous ôte tout souci lié aux spams en les détectant dès réception et en les stockant dans un dossier dédié.

<p><b>Caractéristiques :</b> filtre antispam, tri des messages sans destruction, mises à jour régulières par Internet, compatible <i>Outlook</i>, <i>Outlook Express</i> et <i>Windows Mail</i> sous Windows Me, 2000, XP et Vista.</p>	<p>➔ Efficacité, pas de délai d'attente.</p>	<p>➔ Pas de tri avant réception.</p>	<p>PRIX ■ PERFORMANCES ■ ERGONOMIE ■</p>	<p><b>EN RÉSUMÉ :</b> un bon antispam, capable de s'adapter aux nouvelles techniques de spam.</p>	<p><b>VERDICT</b> <b>08/10</b></p>
---	--	--------------------------------------	--	---	--

**3 questions à Mathieu Tarnus, directeur marketing de Goto Software (1)**

Les éditeurs sont sur tous les fronts pour optimiser leurs solutions anti-spam. Outre les licences, les logiciels desktop, les boîtiers de sécurité déployés chez le client, les entreprises souhaitent également sécuriser leurs flux de messageries avant de les mettre en circulation dans leurs infrastructures. D'où l'émergence, sur le marché de la sécurité informatique, de systèmes de plates-formes hébergées très puissantes mises à disposition des clients, sous différentes formules.



Mathieu Tarnus,  
Goto Software

**- Dans ses argumentaires techniques, Goto insiste sur l'importance de l'analyse du contenu visible/invisible. Pourquoi ?**

Nous croyons en effet aux vertus de la méthode de filtrage heuristique sur l'analyse du contenu des messages (en-tête, corps et objet du message, destinataire, émetteur, balises HTML, scripts...). Une des particularités de notre technologie est d'utiliser le principe des contre-mesures qui vise à détecter dans les messages, les techniques employées par les spammeurs les solutions anti-spam existantes qui utilisent les méthodes de filtrage courantes. Mais si l'analyse de la structure de message est très importante, de même, son contenu invisible l'est tout autant. Dans un message électronique, il existe une structure apparente et une structure cachée, sur laquelle nous nous concentrons beaucoup. Mais, vous le comprendrez, je ne souhaite guère détailler plus avant nos méthodes d'étude et d'analyse.

**- Comment la veille est-elle organisée chez vous ?**

C'est une bonne question dans la mesure où la qualité de la veille est essentielle pour étudier les menaces et les juguler. Nous avons un réseau de 6 ingénieurs qui filtrent et analysent des flux de messageries et nos clients. Nous avons également déployé plusieurs honeypots (pots de miel) sur le web qui nous renseignent précieusement sur les différents types d'attaques par spamming. Avec le temps et l'expérience, nous remarquons qu'il est possible, au moins dans une certaine mesure, de détecter les agissements de plusieurs spammeurs. En effet, bien souvent, ils s'appuient sur d'importants réseaux de machines-zombies. Ces attaques automatiques utilisent souvent un mode opératoire identique qui les rend plus ou moins prévisibles., même si le corps ou les intitulés sont, eux, modifiés très régulièrement afin de traverser les outils de filtrage.

**- Les solutions antispam sont aujourd'hui disponibles sous différentes formes. Quelle est la stratégie de Goto en la matière ?**

Nous maîtrisons le développement de nos solutions logicielles, de nos plates-formes et de notre technologie. Concrètement, nous offrons plusieurs possibilités à nos clients : le déploiement de logiciels desktop avec des contrats de licences, la mise à disposition de boîtiers de sécurité, le recours à des solutions hébergées qui sont aujourd'hui très recherchées et des solutions dites de « librairies techniques » avec des intégrateurs qui sont chargés de mettre en œuvre notre technologie. Ensuite c'est le client qui choisit en fonction de ses besoins et de sa stratégie. Une institution comme les Hôpitaux de Paris souhaite conserver en interne la gestion de ses flux alors que d'autres entreprises, par exemple dans l'industrie, sont très favorables aux solutions hébergées. Dans ce cas, nous collectons et analysons les flux avant de les réacheminer à nos clients. Pour eux, c'est une garantie de sécurité.

<http://www.goto.fr>

Propos recueillis par Gilles PROD'HOMME

(1) Editeur français créé en 1982, Goto Software diffuse une gamme de solutions de protection anti-spam, au travers de sa technologie Vade Retro. La version grand public Vade Retro Outlook et Outlook Express a déjà été téléchargée à plus de 500.000 exemplaires. Goto protège actuellement environ 20 millions de comptes e-mails dans le monde.

### Extension sur le marché nippon

Après un partenariat en Russie, Goto Software a tout récemment signé une alliance avec NetForest dans le but de distribuer les solutions et la technologie Vade Retro auprès des entreprises japonaises. Dans un premier temps, NetForest sera chargée de distribuer la technologie Goto utilisant la méthode de filtrage heuristique, fondée sur l'analyse du contenu des messages (voir « 3 questions à » ci-dessus). NetForest prendra également en charge la distribution de la solution SDK. Intégrable aux systèmes de messagerie, elle permet à chaque message reçu de passer par le programme de traitement, en lui attribuant un score de « spammité ». Le score donne ensuite à l'intégrateur de la technologie, selon les recommandations de la solution SDK, d'entreprendre des actions sur le message lui-même.

## (vulnerabilite.com) Le spam s'écoute maintenant avec le message en pièce jointe au format MP3 !

**BourSoneWS**

18 octobre 2007 (PARIS)

Diffusé par Vulnerabilite.com pour GOTO Software

Le spam s'écoute maintenant avec le message en pièce jointe au format MP3 ! Après les spams images, les spams au formats PDF, XLS... GOTO Software annonce l'arrivée des spams au format MP3 !

Une vague importante de ces nouveaux spams est arrivée cette nuit. Détectés rapidement par le laboratoire Vade Retro, ces messages sont des Pump & Dump, c'est-à-dire des incitations à l'achat d'actions en bourse, au format MP3 en pièce jointe. La société visée par ce spam est EXIT ONLY (EXTO.PK) propriétaire du site text4cars.com. Cette même valeur a déjà été visée par une autre vague en début de semaine mais sous une forme plus courante de propagation. Cette nouvelle vague de spam est d'ores et déjà filtrée par la technologie Vade Retro. Grâce au laboratoire de GOTO Software, tous ses utilisateurs sont protégés et ne subiront aucun désagrément.

A propos de Goto Software Editeur français de logiciel créé en 1982, GOTO Software dispose d'une gamme complète de solutions de protection anti-spam. Spécialiste du filtrage des courriers indésirables en France et en Europe, GOTO Software a développé sa propre technologie : Vade Retro. GOTO Software est capable de répondre aux besoins de protection aussi bien des entreprises que des particuliers. Du boîtier appliance pour salle serveur d'entreprise au logiciel pour poste client, tout a été conçu pour chacun puisse être protégé des spams avec Vade Retro. La version grand public Vade Retro Outlook et Outlook Express a déjà été téléchargée à plus de 500 000 exemplaires. Pour en savoir plus : [www.goto.fr](http://www.goto.fr) / [www.vade-retro.com](http://www.vade-retro.com)

## ITR Manager – 19 octobre 2007

ITR MANAGER.COM

### Le spam arrive au format MP3

 vendredi 19 octobre 2007

On connaissait les spams images, les spams aux formats PDF, XLS, etc. Goto Software annonce désormais l'arrivée des spams au format MP3. Cette vague de spams est arrivée ces derniers jours et a été détectée rapidement par le laboratoire Vade Retro. Les messages concernés sont des Pump & Dump, c'est-à-dire des incitations à l'achat d'actions en bourse, au format MP3 en pièce jointe. La société visée par ce spam est EXIT ONLY (EXTO.PK) propriétaire du site text4cars.com. Ces spams d'un nouveau genre ont d'ores et déjà été filtrés par la technologie Vade Retro.