# Sécuriser les e-mails

## *LIVRE BLANC*

### *LA PREMIÈRE LIGNE DE DÉFENSE STRATÉGIQUE*

# Avertissement

Les informations et les données exposées dans ce document reflètent le point de vue de BitDefender® sur les sujets abordés à la date de sa publication. Ce document et les informations qu'il contient ne peuvent en aucun cas être interprétés comme un engagement ou un accord de quelque nature que ce soit.

Bien que toutes les précautions aient été prises dans l'élaboration de ce document, l'éditeur, les auteurs et les collaborateurs dénient toute responsabilité pour des erreurs et/ou omissions. Pas plus qu'ils n'assument une responsabilité quelconque pour des dommages consécutifs à l'utilisation des informations qu'il contient. De plus, les informations contenues dans ce document sont susceptibles d'être modifiées sans avertissement préalable. BitDefender, l'éditeur, les auteurs et les collaborateurs ne peuvent garantir que ce document sera repris ultérieurement, ni qu'il sera l'objet de compléments ou de mises à jour.

Ce document et les données qu'il contient sont publiés à titre strictement informatif. BitDefender, l'éditeur, les auteurs et les collaborateurs ne donnent aucune garantie expresse, implicite ou légale relatives aux informations mentionnées dans ce document.

Le contenu de ce document peut ne pas être adapté à toutes les situations. Si une assistance professionnelle est nécessaire, les services d'une personne professionnellement compétente doivent être sollicités. Ni BitDefender, ni les éditeurs du document, ni les auteurs ni les collaborateurs ne peuvent être tenus pour responsables des préjudices pouvant résulter d'une telle consultation.

Le fait qu'une personne ou une organisation, un travail individuel ou collectif, y compris des textes imprimés, des documents électroniques, des sites Web, etc., soient mentionnés dans ce document en tant que référence et/ou source d'information actuelle ou future, ne signifie pas que BitDefender, l'éditeur du document, les auteurs ou les collaborateurs avalisent les informations ou les recommandations que peuvent fournir la personne, l'organisation, les travaux individuels ou collectifs, y compris les textes imprimés, les documents électroniques, les sites Web, etc. Les lecteurs doivent également savoir que BitDefender, l'éditeur du document, les auteurs ou les collaborateurs ne peuvent garantir l'exactitude d'aucune des informations données dans ce document au-delà de sa date de publication, y compris, mais non exclusivement, les adresses Web et les liens Internet indiqués dans ce document qui peuvent avoir changé ou disparu entre le moment où ce travail a été écrit et publié et le moment où il est lu.

Les lecteurs ont la responsabilité pleine et entière de se conformer à toutes les lois internationales applicables au copyright émanant de ce document. Les droits relevant du copyright restant applicables, aucune partie de ce document ne peut être reproduite, mise en mémoire ou introduite dans un système de sauvegarde, ni transmise sous aucune forme ni par aucun moyen (électronique physique, reprographique, d'enregistrement, ou autres procédés), ni pour quelque but que ce soit, sans l'autorisation expresse écrite de BitDefender.

BitDefender peut posséder des brevets, des brevets déposés, des marques, des droits d'auteur, ou d'autres droits de propriété intellectuelle se rapportant au contenu de ce document. Sauf accord express de BitDefender inscrit dans un contrat de licence, ce document ne donne aucun droit sur ces brevets, marques, copyrights, ou autre droit de propriété intellectuelle.



Tous les autres noms de produits ou d'entreprises mentionnés dans ce document le sont à titre purement informatif et sont la propriété de, et peuvent être des marques de, leurs propriétaires respectifs.

# Table des matières



# Donnez-nous votre avis

En tant que lecteur de ce document, vous êtes un critique et commentateur essentiel pour nous. Votre opinion nous importe beaucoup et nous serions heureux de savoir ce qui vous plaît dans notre travail, ce que vous n'aimez pas, ce que nous devrions améliorer, quels sujets vous souhaitez nous voir traiter, mais aussi de recueillir tous les autres types de commentaires et suggestions que vous souhaitez partager avec l'équipe BitDefender.

Vous pouvez nous contacter directement par e-mail ou par lettre pour nous dire ce que vous avez trouvé/pas trouvé d'utile et d'intéressant dans ce rapport, et aussi quelles notions et informations nous devrions ajouter pour rendre ce travail plus pertinent.

Dans votre lettre, assurez-vous d'indiquer en référence le titre de ce document et son auteur, ainsi que votre nom, votre numéro de téléphone et votre adresse électronique. Nous étudierons de très près vos commentaires et les transmettrons aux auteurs et aux collaborateurs qui ont travaillé à l'élaboration de ce texte.

Adresse électronique :
documentation@bitdefender.com
Adresse postale :
Editions Profil
49, rue de la Vanne
92120 Montrouge
FRANCE

# *Première ligne de défense stratégique*

Dans le contexte de malveillance qui se développe aujourd'hui rapidement, le cinquième de la population mondiale connectée à Internet doit faire face à environ 2.000 virus nouveaux ou mutés par jour, presque 50.000 tentatives de hameçonnage par mois, et plus de 1.000.000 ordinateurs sont piratés annuellement, propageant bots, rootkits, chevaux de Troie et autres codes malveillants.

Presque 45 % des menaces électroniques circulant dans la nature et harcelant leurs victimes profitent des défaillances humaines et technologiques liées au courrier électronique, ou comptent dans une certaine mesure sur elles.

Le spam est tenu pour responsable de l'augmentation significative des :

- Coûts d'infrastructure – administration du réseau des fournisseurs de services Internet et d'autres entreprises, déploiement de solutions logiciels de filtrage (au niveau ordinateur, serveur, Internet), assistance etc.
- Pertes de productivité – ralentissement des réseaux dû au gaspillage de bande passante, diminution de la rapidité du traitement des e-mails et des capacités de stockage, temps passé à extraire et éliminer les messages non sollicités, et aux effets annexes consommateurs de ressources, par exemple la détection et la suppression des virus transmis par le spam, etc.

En 2005, dans le monde entier, les organisations ont eu à supporter un fardeau financier de 50 milliards de dollars dû aux spams[1]. Pour 2007, les estimations tournaient autour de 198 milliards de coût dû aux courriers non sollicités et aux dégâts qu'ils provoquent[2].

La criminalité électronique cherche à tirer profit de la vulnérabilité des utilisateurs et des systèmes, en adoptant différents types de comportements complexes – et des tactiques et des stratégies axées sur le courrier électronique. La multiplication des connexions Internet à haut débit ces dernières années et le développement spectaculaire des interactions professionnelles quotidiennes par l'intermédiaire des moyens de communication électroniques est un outil idéal et rentable pour la circulation des idées, mais également pour la dissémination des menaces électroniques.

Dans ce contexte, la sécurisation des communications électroniques doit devenir une priorité en termes de :

- Protection des biens, des idées et des données sensibles
- Sauvegarde de l'intégrité des réseaux des entreprises
- Evaluation et renforcement des normes, des règlements, de la gestion des risques et de la conformité
- Défense des investissements et réduction du coût total de possession.

Ce document expose le problème de la sécurité du courrier électronique en insistant sur les mécanismes psychologiques sous-jacents dans les menaces actuelles sur Internet. Des statistiques et des faits aideront les lecteurs à appréhender le phénomène de leur propagation à partir de données quantitatives.

Les ripostes aux menaces qui sont alors traitées indiquent précisément les armes de dissuasion utilisées et les résultats visés en termes de sécurité des serveurs de messagerie. Ce document a pour objectif de donner à ses lecteurs les moyens de mettre en pratique une politique de prudence dans les communications électroniques permettant une administration efficace des ressources réseaux.

---

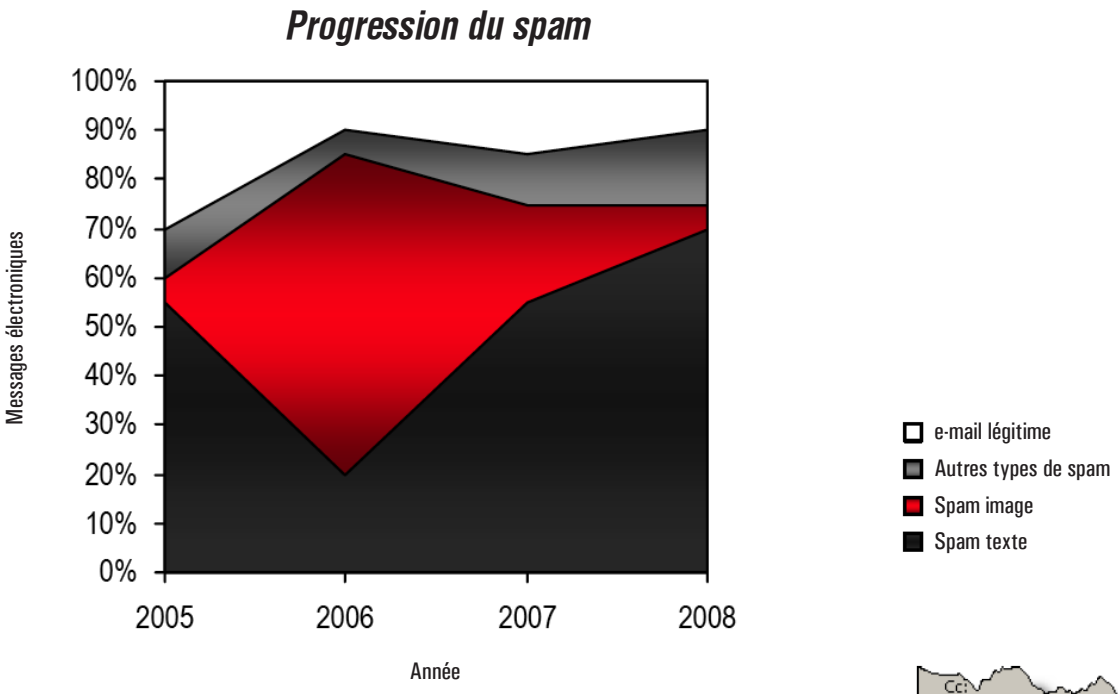
[1] David Ferris, Richi Jennings, Chris Williams, "The Global Economic Impact of Spam, 2005. Report #409. Ferris Analyzer Information Service", publié le 24 février 2005, sur Ferris Research, http://www.ferris.com/2005/02/24/the-global-economic-impact-of-spam-2005/.

[2] ACitation de Robert Jaques, "Spam will cost business $20.5bn this year", publié le 10 juin 2003, sur Incisive Media's www.vnunet.com, http://www.vnunet.com/vnunet/news/2122506/spamcost-business-5bn.

# Sécurité électronique : Menaces et tendances actuelles

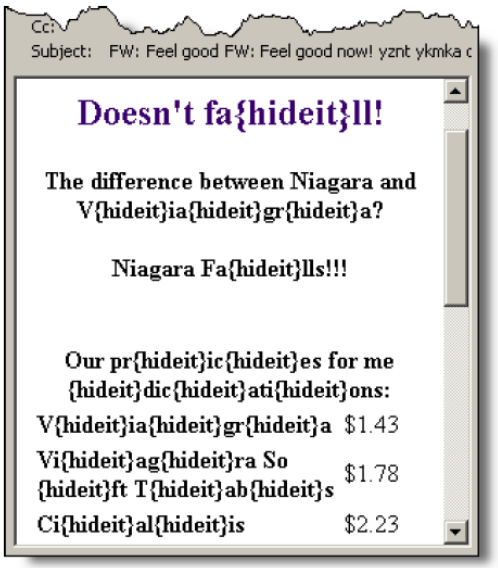
Cette partie du document donne les statistiques relatives aux types de spam et de virus, et décrit les différents stratagèmes à l'origine de leur propagation. Elle s'intéresse également au facteur humain ciblé dans chaque attaque, et expose dans quelles circonstances psychologiques, techniques et sociales de telles attaques peuvent se produire et triompher.

Concernant les supports et les techniques du spam, la tendance la plus notable au premier semestre 2008 est la résurgence du spam texte, qui a atteint cette année 70 % (contre 20 % au cours de la même période en 2007). Le déclin du spam image se poursuit, et n'atteignait plus que 3 % au milieu de l'année 2008 (contre 60 % l'an dernier)[3].




Le message textuel demeure le support de spam le plus prolifique. Ceci s'explique notamment par sa simplicité, sa taille réduite et son extrême versatilité.

Ce type de spam se prête bien aux scripts automatiques de brouillage de mots, de reformulation ou de substitution (synonymique). Par contre, le spam image utilise généralement un contenu brouillé. D'autres catégories de spam, par exemple les courriers auxquels sont joints des fichiers PDF, audio, vidéo, etc. ont progressivement perdu de leur popularité et ont finalement disparu. Leur part de 10% à 15 % a été remplacée par des messages combinant du texte ou du HTML.



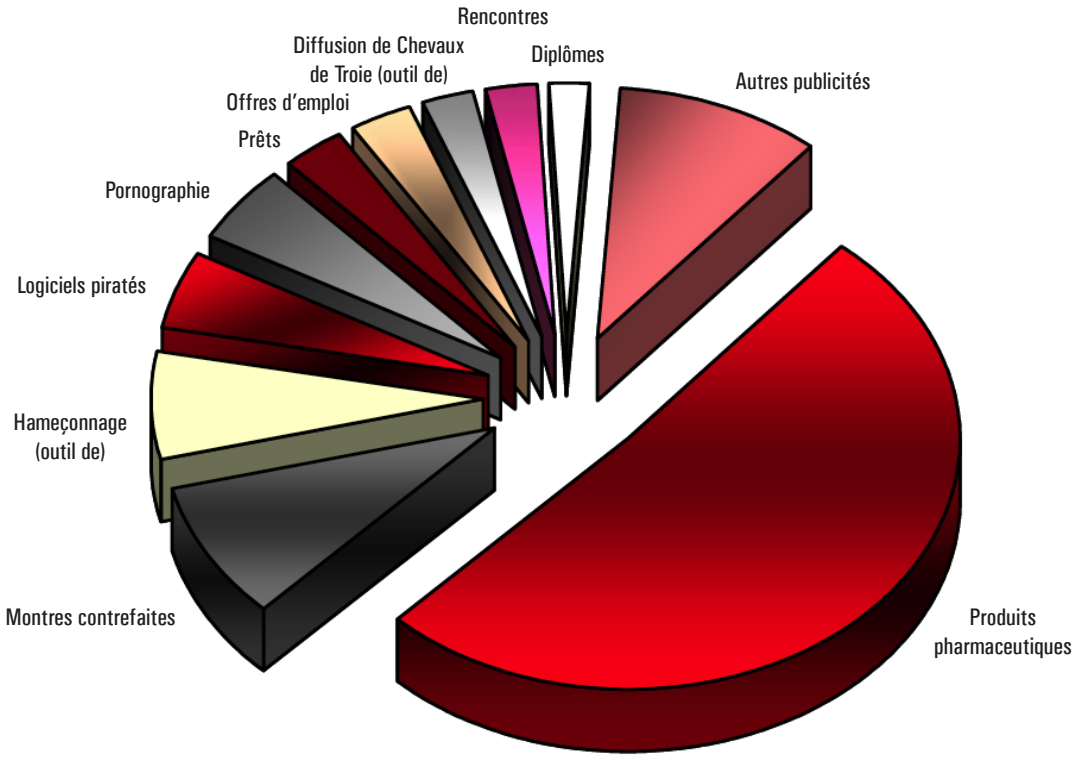

[3] Voir «E-Mail Spam Morphs in First Half of 2008», publié le 3 juillet 2008, dans BitDefender, http://news.bitdefender.com/NW764-en--E-Mail-Spam-Morphs-in-First-Half-of-2008.html.

Les spams contenant des informations boursières sont en perte de vitesse. La seconde moitié de l'année 2007 a été dominée par le spam contenant des images et des fichiers audio .mp3. Par contre, au cours des six premiers mois de 2008 on a pu constater le retour des spams à messages textuels en clair.

Le Top 10 des spams de la première moitié de 2008 trié par contenu

### Contenu principal du spam
### Janvier à juin 2008

| RANG | CONTENU TYPE | Pourcentage |
|---|---|---|
| 01. | Produits pharmaceutiques | 51 |
| 02. | Montres contrefaites | 9 |
| 03. | Hameçonnage (outil de) | 7 |
| 04. | Logiciels piratés | 5 |
| 05. | Pornographie | 5 |
| 06. | Prêts | 3 |
| 07. | Offres d'emploi | 3 |
| 08. | Diffusion de Chevaux de Troie (outil de) | 2.5 |
| 09. | Rencontres | 2.5 |
| 10. | Diplômes | 2 |
| 11. | Autres publicités | 10 |




En matière de prévention antispam, les dernières tendances consistent à profiter des anomalies/failles de la messagerie (ce qui rend difficile de déverrouiller les mails pour les examiner), et à utiliser un code HTML corrompu destiné à brouiller les analyseurs. Par contre, l'intoxication du filtre de Bayes (brouillage des filtres antispam utilisant un dictionnaire par l'ajout de mots et de phrases aléatoires à un courrier électronique) et l'altération de mots (en écrivant par exemple «SP4M» au lieu de «spam») semble être de moins en moins pratiquée.

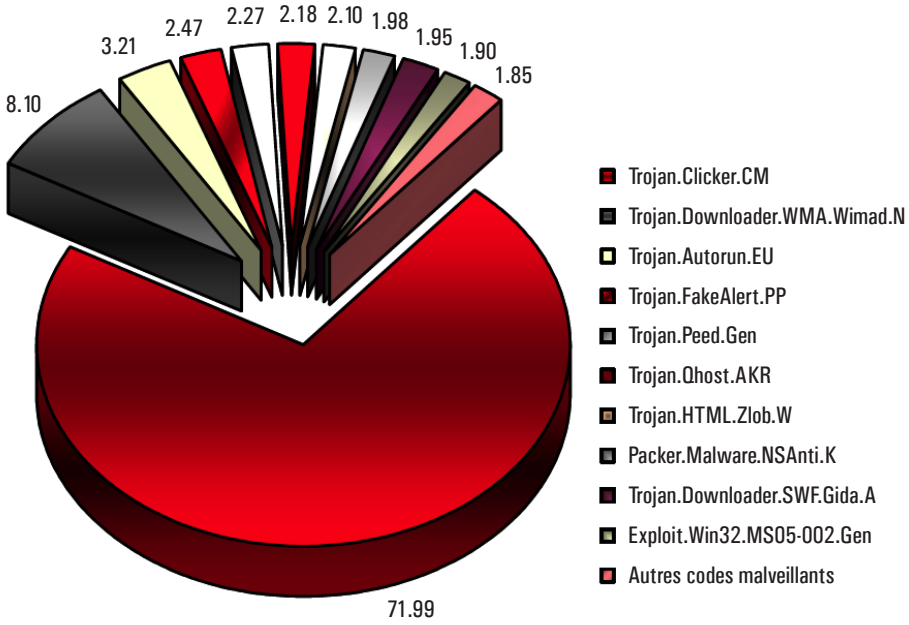
Les six premiers mois de 2008 ont montré que les concepteurs de codes malveillants concentraient désormais leurs efforts à exploiter la vulnérabilité des systèmes en se faisant passer pour des applications légitimes. Ainsi, les chevaux de Troie constituent 80 % de la courbe des types de codes malveillants.[4]

La cuvée 2008 du code malveillant continue de tourner autour du profit, principalement financier. Pour augmenter leurs gains, les cybercriminels doivent trouver le moyen de compromettre un très grand nombre de systèmes où déployer le plus de bots, adware et spyware possible, à moindre frais, ou sans frais du tout. Ainsi, l'activité principale n'est plus de disséminer le code malveillant, mais d'infiltrer les systèmes et de les rendre vulnérables à d'autres menaces. Ceci explique la production de masse de chevaux de Troie ces dix derniers mois. Les chevaux de Troie, qui téléchargent d'autres types de code malveillants, comme le spyware, l'adware, les rootkits, etc, et «ouvre les portes» des machines infectées, constituent un risque majeur. Les programmes spyware enregistrent subrepticement l'activité de l'utilisateur et recueillent ses données, à la recherche de celles qui lui sont personnelles (comme le numéro de ses cartes bancaires ou le mot de passe qu'il utilise pour ses comptes en ligne). Ce sont en somme de sinistres services d'indexation.

Le Top 10 des codes malveillants les plus efficaces pour la première moitié de 2008 comprend :

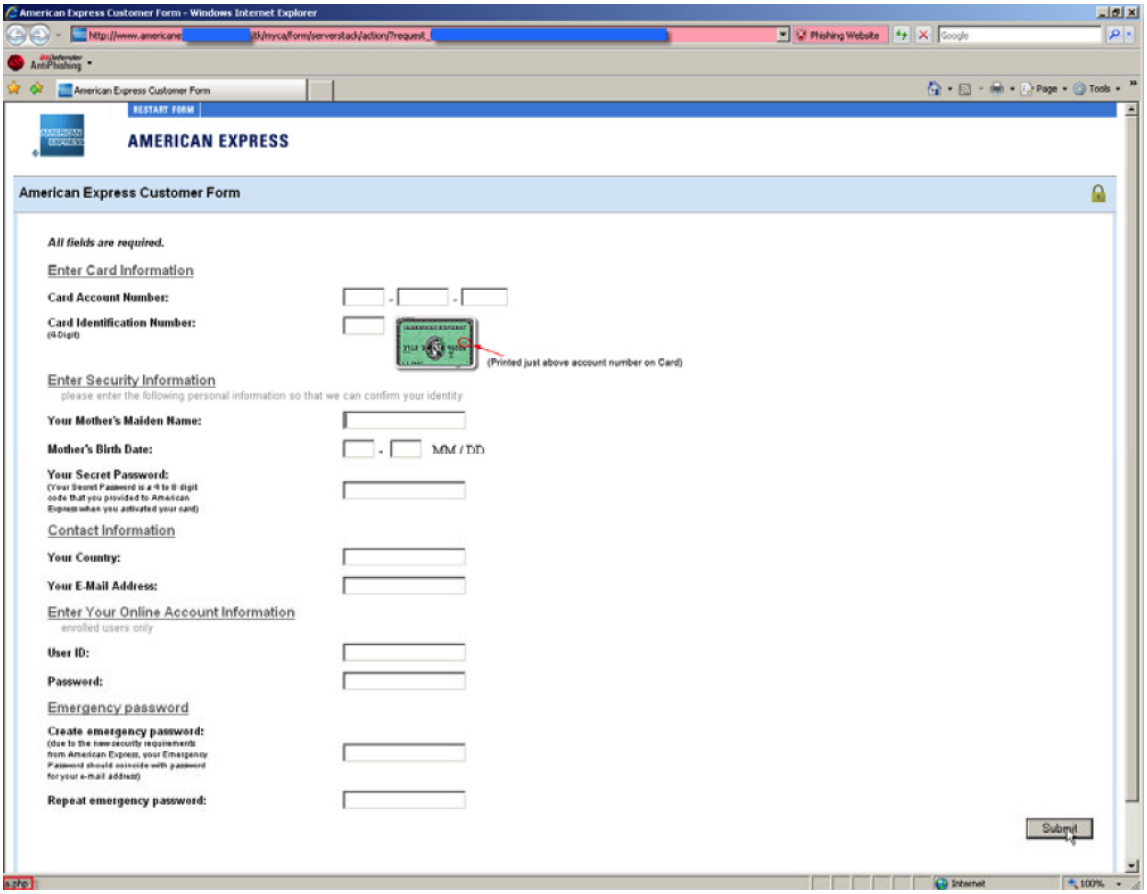
### Top 10 mondial des codes malveillants, de janvier à juin 2008

| RANG | Code malveillant | Pourcentage |
|---|---|---|
| 01. | Trojan.Clicker.CM | 8.10 |
| 02. | Trojan.Downloader.WMA.Wimad.N | 3.21 |
| 03. | Trojan.Autorun.EU | 2.47 |
| 04. | Trojan.FakeAlert.PP | 2.27 |
| 05. | Trojan.Peed.Gen | 2.18 |
| 06. | Trojan.Qhost.AKR | 2.10 |
| 07. | Trojan.HTML.Zlob.W | 1.98 |
| 08. | Packer.Malware.NSAnti.K | 1.95 |
| 09. | Trojan.Downloader.SWF.Gida.A | 1.90 |
| 10. | Exploit.Win32.MS05-002.Gen | 1.85 |
| 11. | Autres codes malveillants | 71.99 |




[4] Voir «BitDefender Lab Publishes first E-Threats Landscape Report», publié le 30 juillet 2008, dans BitDefender, http://news.bitdefender.com/NW795-en--BitDefender-Lab-Publishes-first-E-Threats-Landscape-Report.html.

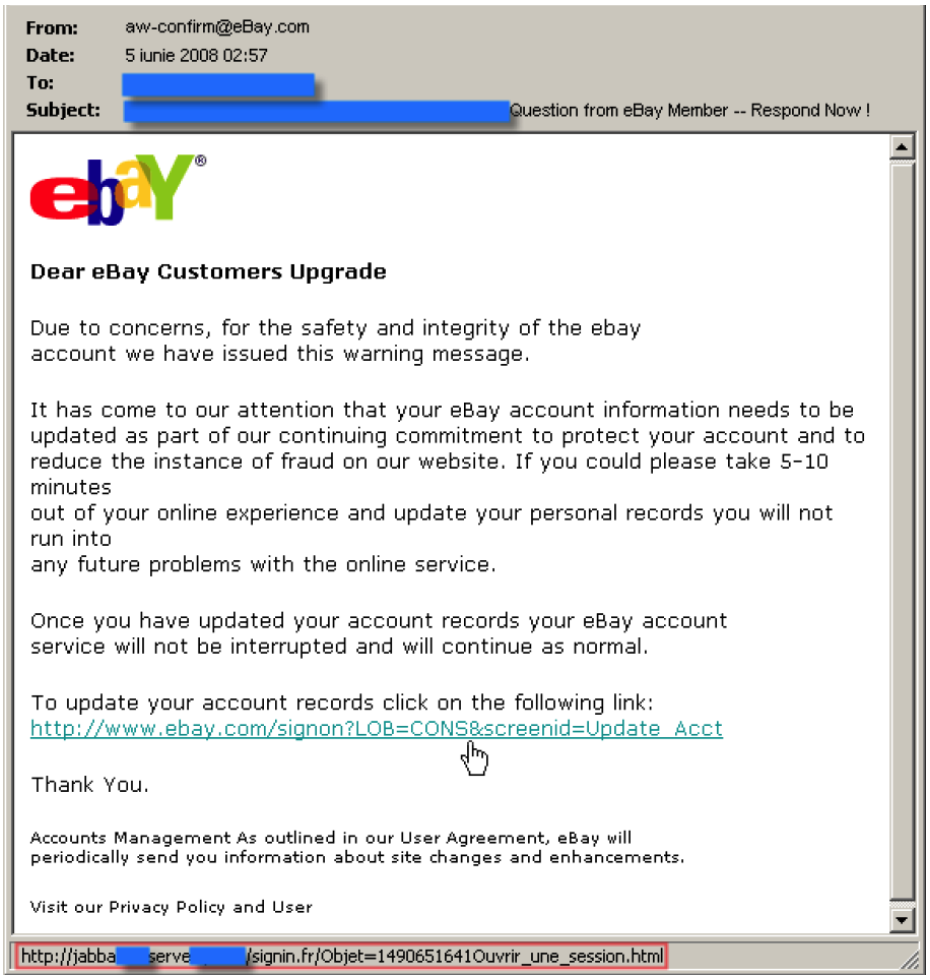
Cependant, un autre moyen de recueillir des informations personnelles est d'envoyer des courriers électroniques censés provenir d'institutions financières (légitimes) demandant simplement ce type de renseignements. Ces courriers de type « hameçonnage » contiennent généralement des liens vers des sites Web contrôlés par le fraudeur, mais que rien ne permet de distinguer des sites authentiques sans l'aide de logiciels de sécurité. La détection de tels courriers s'effectue principalement grâce aux techniques fondées sur des règles (heuristiques) comme le filtrage des liens (vérification que les liens dans le courrier pointent sur la vraie cible – dans l'image ci-dessous, derrière le bouton Soumettre, se trouve le script a.php qui va voler les données sensibles) ou le filtrage d'images (ces fraudeurs utilisent le logo d'organismes financiers pour rendre leurs courriers crédibles).




Les tendances du hameçonnage pour la première moitié de 2008 révèlent une évolution et une augmentation des entreprises factices et des clients ciblés. Les fraudes ont d'abord concerné les organismes financiers américains, tandis que les victimes potentielles sont maintenant les anglophones résidant aux Etats-Unis, au Royaume Uni ou au Canada, bien que les chercheurs de BitDefender aient reçu des informations d'Espagne, d'Italie et de France sur des attaques en cours.

Les activités de hameçonnage sont basées sur un modèle simple. En général, les fraudeurs font déferler des vagues de spams pour piéger les destinataires (ceux qui utilisent les services en ligne des banques) et les inciter à communiquer des informations privées. Le message a l'air d'être envoyé par l'organisme financier, et suggère au client d'utiliser un lien ou d'ouvrir une page Web attachée.

La plupart des arguments invoqués dans les messages illégitimes sont défavorables : blocage ou fermeture de compte, augmentation des frais d'agios, ou mise à jour des coordonnées du compte pour des raisons de sécurité. D'autres méthodes de faire «mordre à l'hameçon» tablent sur des incitations favorables, par exemple la perspective de bénéficier d'une certaine somme si l'utilisateur remplit toutes les rubriques d'un questionnaire en ligne ou attaché.




**Le Top 10 des identités commerciales falsifiées pendant la première moitié de 2008 comprend :**

1. eBay
2. Paypal
3. Bank of America
4. Wachovia
5. Fifth Third Bank
6. NatWest
7. Poste Italiane
8. Sparkasse
9. Regions Bank
10. Volksbank

Spammeurs et fraudeurs par hameçonnage continuent d'améliorer leurs talents dans le domaine de la copie et de l'élaboration des caractéristiques de messages légitimes. Cependant de simples textes envoyés par courriers électroniques prouvent également leur efficacité, le chiffre total des victimes de vol d'identité avoisinant les 50.000 par mois.

Pourquoi certains deviennent-ils les victimes du hameçonnage ou de codes malveillants ? Qu'est-ce qui les pousse à cliquer sur ce lien fatal ou à lancer cet exécutable véreux ?

# Vecteurs comportementaux des attaques

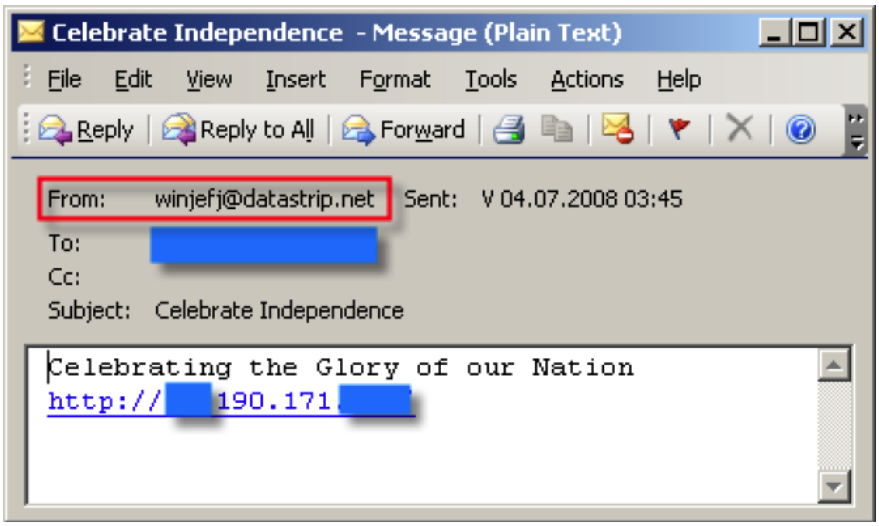
Cette section répertorie quelques-uns des principaux vecteurs qu'exploitent les pirates pour mettre en péril ou contrôler l'ordinateur des utilisateurs, voler des données et de l'argent :

- Le divertissement
- La curiosité
- L'empathie
- La cupidité

## Le divertissement

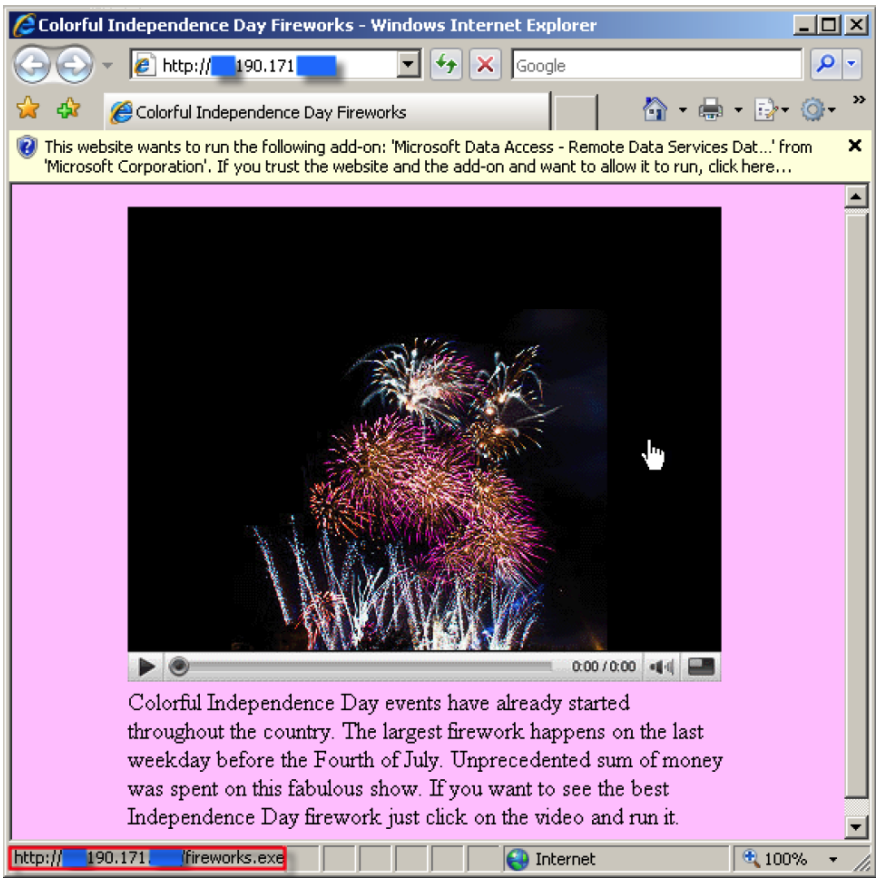
Le code malveillant fructueux se dissimule sous l'aspect de «plaisanteries», avec les conséquences que l'on a connues il y a quelques années, ou «d'images de vacances» publiées chaque année. Ce vecteur est assez fructueux puisque chaque année pendant la période des congés, ou quand se produit un événement important, de nouvelles vagues de codes malveillants et de spam déferlent.

Par exemple, le 232ème anniversaire de l'Indépendance américaine a été marqué par une vague significative importante de spam. Le spam en lui-même était inoffensif, et son texte anodin, imitant celui des messages que les gens échangent ou se transmettent habituellement à cette occasion. Il était constitué d'une seule ligne de texte (sans aucun document joint), suivie d'un lien vers un site Web comme dans la saisie d'écran ci-dessous.




Le seul élément suspect était l'adresse électronique (probablement générée automatiquement) derrière le nom de l'expéditeur, qui pouvait alerter sur la nature malveillante du message.

Sélectionné, le lien hypertexte conduisait à une page Web affichant une fenêtre contenant un faux lecteur vidéo et un message sur l'un des plus grands des feux d'artifice du 4 juillet, comme on le voit dans l'image qui suit :




Une fois ouverte, la page essayait automatiquement de lancer et d'installer à distance un script Java avec plusieurs couches de données cryptées – le Trojan.JS.Encrypted.A. Ce cheval de Troie utilise un esclave (exploit) pour exécuter le code crypté du shell.

En outre, quand on cliquait dans la fenêtre du faux lecteur, le navigateur téléchargeait et installait automatiquement un fichier nommé fireworks.exe (au lieu de passer un film). Cet exécutable ne renfermait aucun contenu de type multimedia compressé ou se lançant automatiquement, mais uniquement un autre virus – Trojan.PEED.JLV possédant ses propres mécanismes malveillants de multiplication et de distribution.

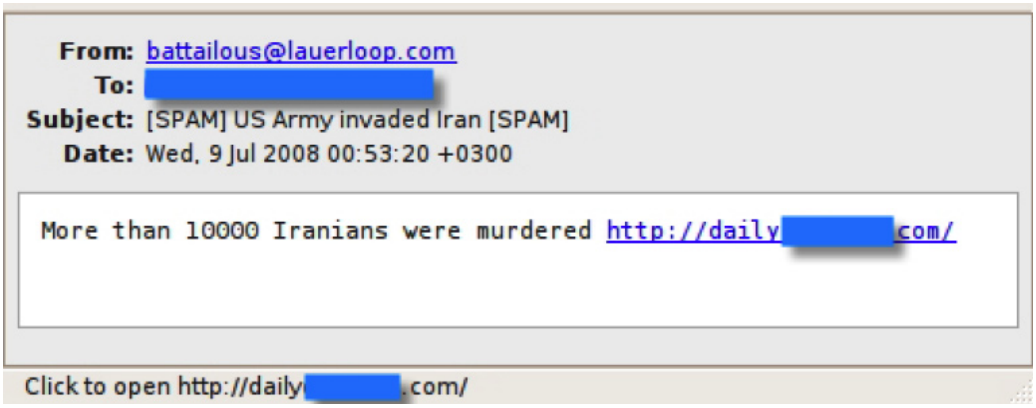
Lorsqu'il envahit un système, le cheval de Troie se copie lui-même dans le dossier du système d'exploitation et modifie les paramètres du pare-feu Windows. En outre, il enregistre l'ordinateur atteint en tant que pair dans son réseau malware et utilise un port choisi au hasard pour communiquer avec les autres pairs et mettre à jour sa liste de ces derniers.

Le virus Peed recherche des adresses électroniques sur tous les disques locaux et s'envoie lui-même sous l'aspect du spam précédemment décrit, en utilisant généralement l'adresse électronique de l'hôte. Parmi les textes possibles en Objet : «Célébrez l'Indépendance», «Anniversaire de l'Indépendance - Feux d'artifice», «Etonnants Feux d'artifice 2008», «Le pays de la liberté», etc.

## *La curiosité*

Le désir de voir des photos de célébrités ou des films de nouvelles catastrophes naturelles ou d'événements violents peut pousser à des actes irréfléchis.

Dans l'exemple qui suit, une grande marée de messages spam annonçant une prétendue attaque de l'armée américaine contre l'Iran, était destinée à piéger les usagers et les conduire à télécharger et installer des logiciels malveillants sur leurs ordinateurs personnels.




La page Web hébergeant le code malveillant était effectivement bien conçue, avec un titre, une image censée représenter un lecteur YouTube et quelques lignes décrivant la prétendue l'intervention américaine en Iran. Cette approche est utilisée à grande échelle, les spammeurs comptant sur un titre accrocheur et un lien vers le code malveillant pour attiser la curiosité des utilisateurs et les amener à mettre leurs machines en danger.


En cliquant sur «le film» ou le bandeau, l'utilisateur faisait démarrer le processus de téléchargement d'un code binaire malveillant, nommé iran_occupation.exe. Le fichier contenait le même code malveillant utilisé pour infecter les utilisateurs avec le vers Storm. Socialement parlant, la vague de spam visait à profiter de l'inquiétude des citoyens américains, soucieux d'obtenir des informations sur les menaces de l'Iran de détruire Tel Aviv en cas d'attaque éventuelle de ses installations nucléaires par les Etats-Unis.

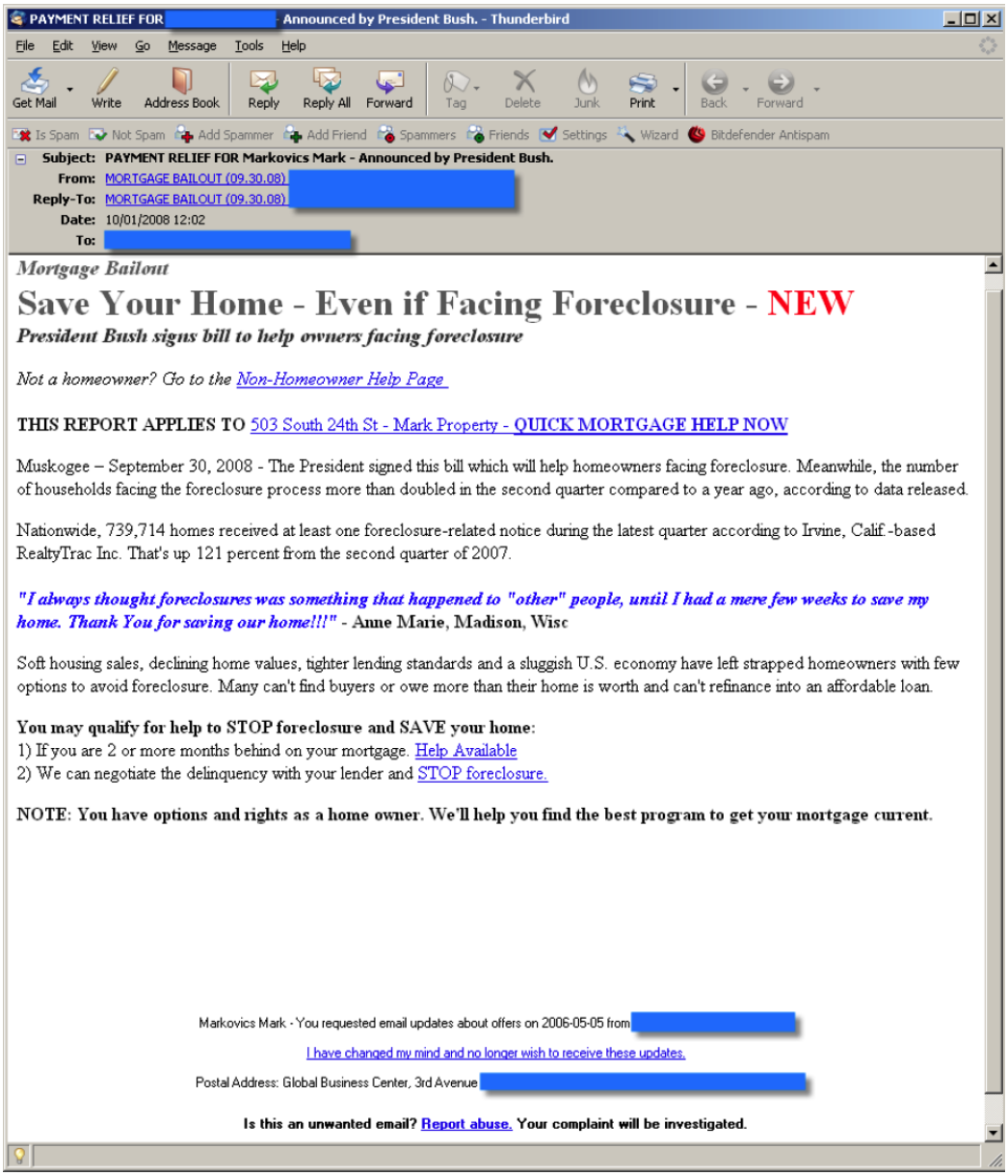
## *L'empathie*

Les appels aux dons, au bénévolat, au soutien de nobles causes dominent déjà les rubriques électroniques. Comment faire la différence entre des demandes caritatives honnêtes et celles sans scrupule des escrocs ?

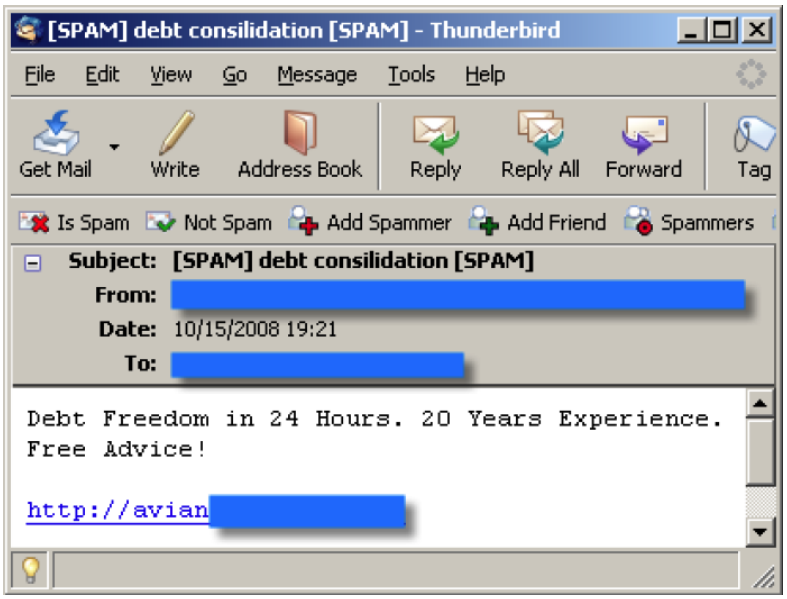
Les exemples qui suivent illustrent bien la question : au moment où le système financier mondial pourrait perdre 2.800 milliards de dollars pendant la récession, l'industrie du spam pourrait terminer 2008 avec un résultat positif.

L'effondrement initial mi-septembre des principales banques et compagnies d'assurance n'annonçait pas seulement la dépression imminente ; il laissait également prévoir l'accroissement du spam qui a suivi. Spéculant sur l'anxiété générale, qui a tourné début octobre à la panique totale quand les bourses du monde entier se sont effondrées, les spammeurs ont essayé de séduire leurs destinataires en leur proposant des services prétendant pouvoir éliminer ou réduire les dettes, les emprunts, et autres obligations fiscales.

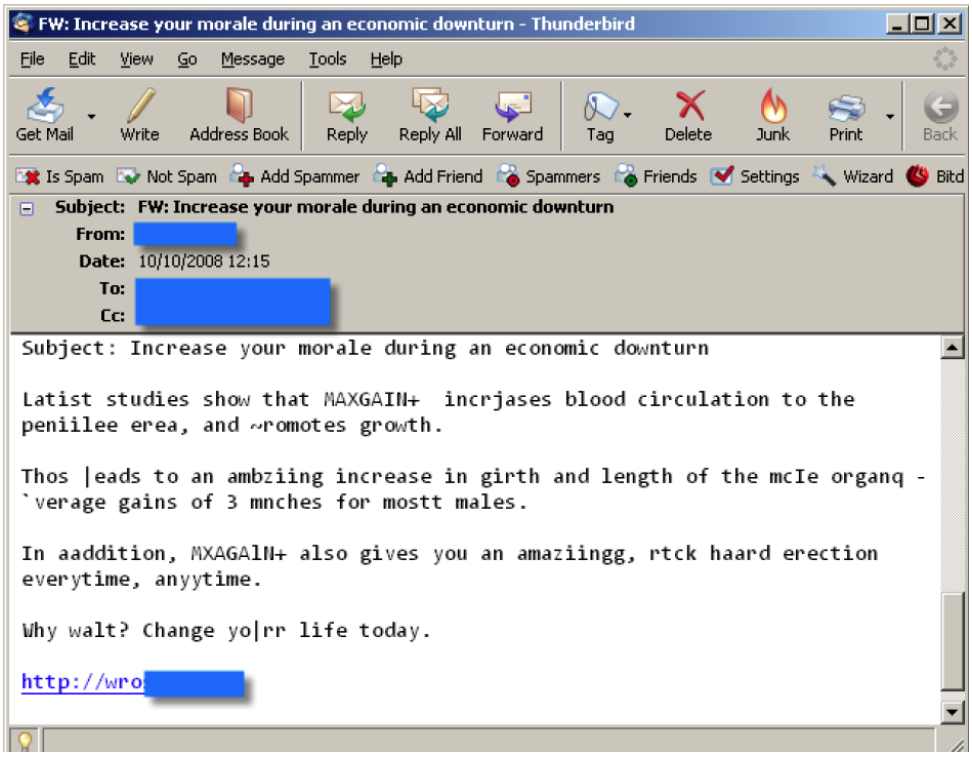
Une importante vague de spams ayant pris pour cible les habitants des Etats-Unis a fait la publicité des services d'une société qui prétendait pouvoir empêcher la saisie des maisons hypothéquées. Comme décrit ci-dessous, le message jouait sur le dernier plan de sauvetage annoncé par le Président Bush.



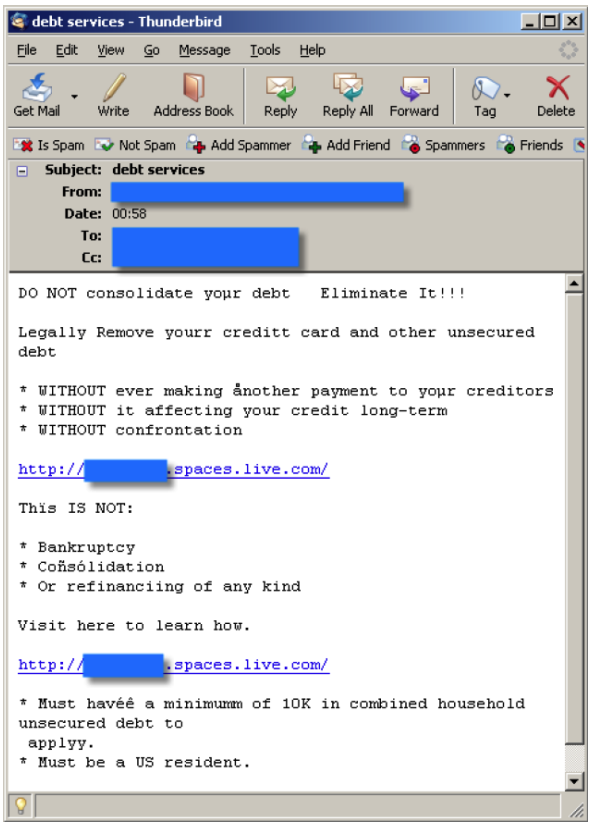

A partir d'un modèle utilisé avant la récession, de nouvelles campagnes ressemblant à des publicités financières ont pris une extension significative au cours des deux derniers mois. Généralement limité, dans le texte ou l'objet, à une seule ligne susceptible d'allécher les destinataires, ces messages proposaient des liens conduisant les utilisateurs vers différents sites Web, dont beaucoup sont probablement impliqués dans des programmes de hameçonnage.

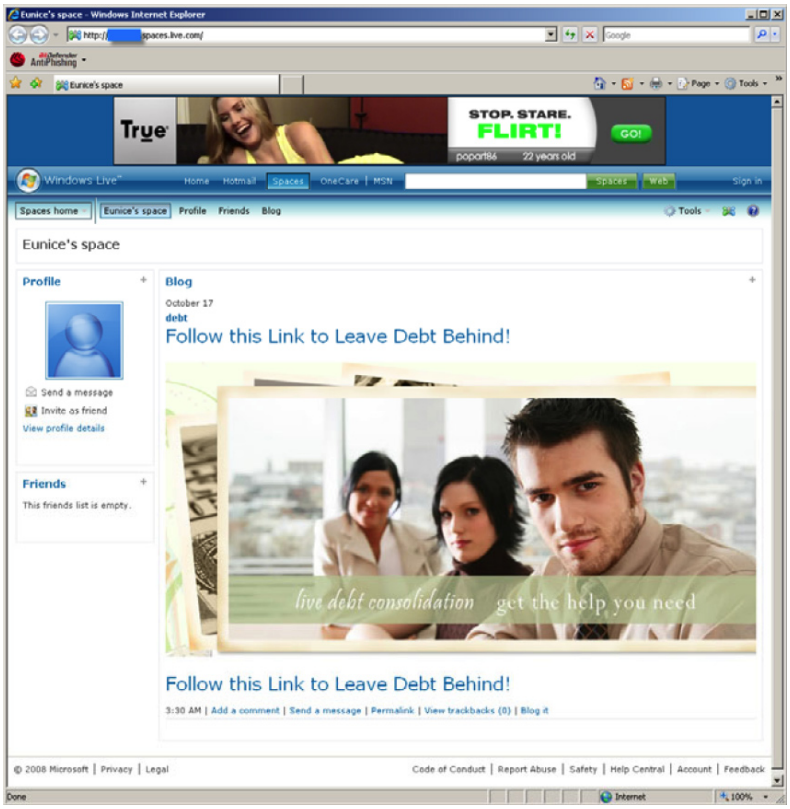



D'autres vagues de spams ont profité de la crise économique pour faire de la publicité sur les produits pharmaceutiques, les logiciels piratés et les articles contrefaits. Le message ci-dessous par exemple, fait la promotion d'un antidote à la dépression – une drogue censée améliorer la vie sexuelle.




Enfin, l'une des plus récentes tentatives du spam reposait sur une multitude de combinaisons de courriers générés et distribués automatiquement et de profils sociaux. Leur objectif était de diriger les destinataires vers des sites Web où ils seraient censés pouvoir « laisser leur dette derrière eux ».

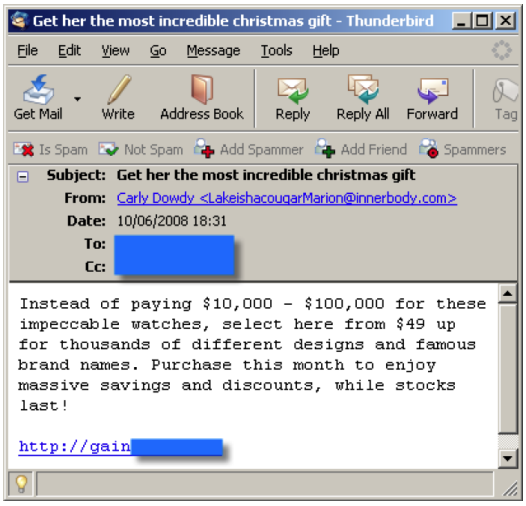

debt services - Thunderbird
File Edit View Go Message Tools Help
Get Mail Write Address Book Reply Reply All Forward Tag Delete
Is Spam Not Spam Add Spammer Add Friend Spammers Friends
Subject: debt services
From:
Date: 00:58
To:
Cc:
DO NOT consolidate your debt Eliminate It!!!
Legally Remove yourr creditt card and other unsecured debt
* WITHOUT ever making another payment to your creditors
* WITHOUT it affecting your credit long-term
* WITHOUT confrontation
http://.spaces.live.com/
This IS NOT:
* Bankruptcy
* Coñsólidation
* Or refinancing of any kind
Visit here to learn how.
http://.spaces.live.com/
* Must havéé a minimumm of 10K in combined household unsecured debt to
applyy.
* Must be a US resident.


Eunice's space - Windows Internet Explorer
STOP. STARE. FLIRT!
GO!
Eunice's space
Profile
Blog
October 17
debt
Follow this Link to Leave Debt Behind!
live debt consolidation get the help you need
Follow this Link to Leave Debt Behind!

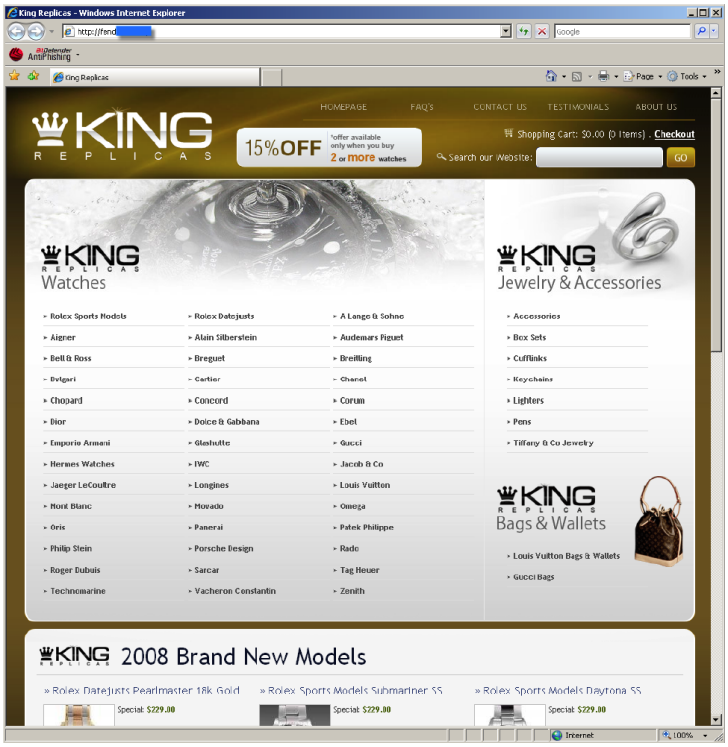
## La cupidité

La cupidité est le vecteur comportemental le plus stable. Tant qu'il y aura des marchés, une tension existera entre le besoin du producteur de faire un profit et le besoin de l'acheteur «d'avoir cette chose». L'impossible équilibre entre ces deux souhaits laisse aux criminels un fossé à combler en utilisant le vecteur «cupidité».

Par exemple, la campagne de spam qui suit faisait la publicité pour des contrefaçons de montres et de bijoux que l'on pouvait acheter en ligne, tout en soi-disant pouvoir «profiter de remises massives» :




Le lien hypertexte dirigé ver le site Web « bling-bling » de King Replica, élément clé d'une fraude plus élaborée offrant une parfaite couverture pour le vol d'identité et d'autres données sensibles (comme les numéros de cartes bancaires). Outre les prix élevés demandés pour de médiocres imitations, le site Web affichait l'avertissement suivant sous la rubrique Terms and Conditions : « Nous ne donnons aucune garantie pour aucun des produits vendus sur commandes effectuées sur ce site. Ces produits de très bonne qualité sont des articles de fantaisie ».



Les attaques utilisant ce vecteur vont de la plus simpliste – comme le type de spam nigerian aux tentatives les plus sophistiquées de hameçonnage ou de fraudes financières, qui englobent aussi les ventes au rabais de publications, produits pharmaceutiques, logiciels ou produits de luxe.

Ces attaques sont économiquement très rentables, dans la mesure où les technologies de communication actuelles permettent la diffusion de contenu pour un coût avoisinant le zéro, mais ne permettent pas à coup sûr d'identifier les diffuseurs de contenu. Le coût (et le risque) encouru pour l'agression d'une seule personne n'est pas significativement plus faible que celui encouru pour l'agression d'un millier d'autres, alors que l'émergence d'un vaste réseau public de bases de données d'informations personnelles permet aujourd'hui de cibler de telles attaques comme jamais auparavant. Un fraudeur peut cibler les clients connus d'une banque donnée dans une zone géographique particulière et préparer des attaques sur mesures (du choix du message à celui des serveurs à pirater ou mettre hors service) en fonction des critères retenus.

## Vecteurs technologiques des attaques

Il n'existe qu'un vecteur en ce qui concerne les technologies que nous utilisons : l'exploitation fondée sur les failles des logiciels. Ces défauts peuvent se classer en deux catégories : erreurs de conception et erreurs d'implémentation, elles-mêmes se subdivisant en débordements de la pile et tampons, injection et exécution de scripts, déni de service, attaque du type « man-in-the-middle » et une kyrielle d'autres types d'attaques.

Les réalités de la concurrence économique entre éditeurs de logiciels, l'imperfection des méthodes et des outils de développement, voire les défauts ou les incohérences des systèmes utilisés pour concevoir les logiciels, concourent à rendre impossible le développement de logiciels ne contenant pas de bogues.

Le logiciel vulnérable le plus répandu est celui qui intéresse le plus les attaquants. Un produit qui rencontre du succès est une cible facile, le coût que représente la recherche d'un défaut et son exploitation étant largement compensé par les gains à obtenir d'un vaste réservoir de victimes – les utilisateurs du logiciel. Une fois un défaut détecté, le processus d'écriture et de déploiement de son exploitation est très simple et peut même être en partie automatisé. Malheureusement, le courrier électronique est l'un des vecteurs privilégiés et les serveurs de messagerie non sécurisés ou mal configurés sont au coeur de la stratégie des pirates : leur incapacité à fonctionner en tant que gardiens se traduit par plus d'argent pour les criminels.

## Perspectives sociales

Un nouveau modèle se dessine dans l'activité hautement illégale et profitable de la création et de la diffusion de codes malveillants.

Avec l'apparition de solutions de sécurité pour serveurs extrêmement efficaces, les «clandestins» doivent s'organiser de manière plus sophistiquée pour exercer un meilleur contrôle des ressources logicielles et matérielles accumulées par chaque fraudeur. Nous sommes probablement en train d'atteindre un point d'équilibre, où les ressources des grandes organisations criminelles vont se mesurer à celles du même ordre des entreprises et des gouvernements. Ce conflit est le premier de l'histoire mondiale à être alimenté par des logiciels – codes malveillants d'un côté et logiciels de sécurité de l'autre.

Les criminels exploitent les infrastructures existantes (communications et informatique) pour perpétrer leurs délits tout en les rendant moins utilisables. Bien que la résistance reste ferme (efforts accomplis dans la lutte anti-codes malveillant et anti-spam), criminels et organisations légitimes continuent à profiter de cette infrastructure. Si jamais les criminels l'emportaient, l'infrastructure pourrait devenir inutilisable (d'après des chiffres récents, le spam constitue 80-90 % du courrier électronique) et abandonnée au profit d'autre chose.

Dans le but de mieux contrecarrer l'augmentation des codes malveillants, la société s'emploie à imposer des lois susceptibles de réduire le flux monétaire vers cette économie parallèle. Les lois liées à la sécurité informatique se renforcent avec des pouvoirs d'intervention de plus en plus importants, et les officiers de police sont désormais entraînés, dans le monde entier, à combattre cette nouvelle forme de criminalité.

## Dépasser le stade "roue de la fortune"

Ce chapitre du document contient une liste d'arguments venant appuyer l'utilisation d'une solution de sécurité pour la messagerie, pour supprimer tous les obstacles entravant la voie vers une communication électronique sans conflits pour les PME. Il décrit également le concept de sécurité des serveurs de messagerie en mettant l'accent sur les aspects particuliers des PME au moment de prendre une décision dans ce domaine.

## Logiciels de sécurité : Le pourquoi et le comment

En définitive, quelqu'un peut-il dire pour quelles raisons les entreprises doivent avoir recours à une solution de sécurité pour serveur de messagerie ? En fait, oui. C'est un choix qui s'inscrit de plus en plus dans les «pratiques courantes» de l'univers des communications électroniques actuelles et il est dicté par le besoin de toujours avoir une longueur d'avance sur le développement des menaces en ligne.

Ce choix est fondé sur quelques réalités qui se rattachent aux deux principaux problèmes de sécurité qui peuvent toucher les réseaux d'entreprises : les virus et le spam. Les solutions de sécurité préservent la stabilité de l'infrastructure informatique, tout en diminuant le risque d'infection des destinataires des messages. En outre, de nouvelles technologies de protection, inspirées par la recherche en IA, sont capables d'inverser le courant et de fournir un niveau de sécurité sans précédent, en détectant et neutralisant rapidement les menaces nouvelles et inconnues jusque là. Les solutions de sécurité conçues pour filtrer et bloquer le spam permettent également une utilisation plus efficace de la bande passante et de l'espace de stockage. En vérifiant le contenu de ce qui sort du système elles aident au maintien de la confidentialité de la correspondance professionnelle en supprimant le risque du vol de données sensibles.

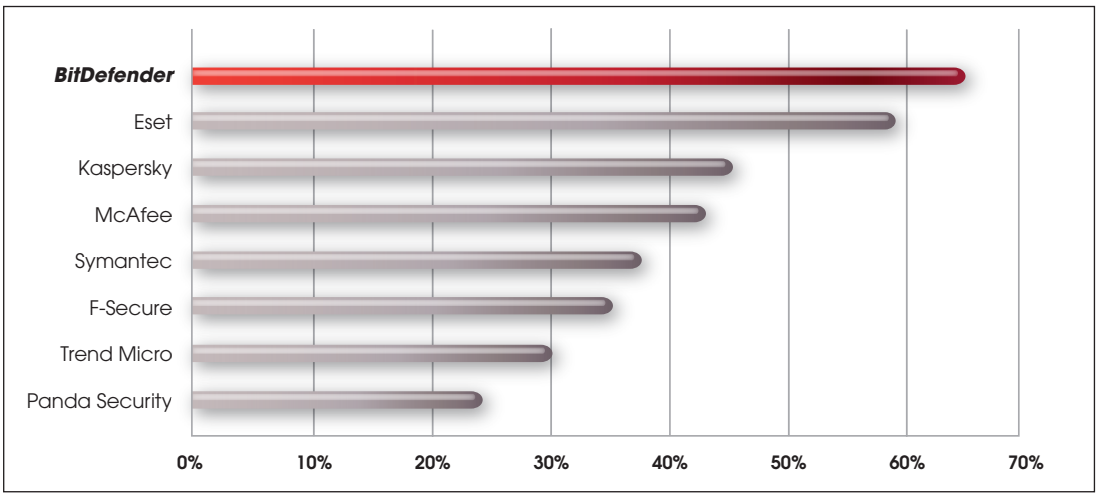
Un exemple des produits conçus en tenant compte de tous ces impératifs est la série de solutions pour serveurs de BitDefender. Elle rassemble antivirus, antispyware, antispam, anti-hameçonnage, et la possibilité de filtrer documents attachés et contenu, pour créer à l'intention des grandes comme des petites entreprises un environnement dépourvu de codes malveillants.

## Protection proactive

La protection des données doit s'exercer dans deux directions. Regarder derrière soi peut permettre de recueillir des informations sur la structure et le comportement de codes malveillants, informations qui peuvent être utilisées ensuite pour s'opposer à la récurrence des mêmes attaques. C'est ainsi que fonctionnent les méthodes basées sur les signatures. Mais les entreprises doivent aussi rester attentives et regarder vers l'avant, dans la mesure ou de nouveaux types de codes malveillants apparaissent à un rythme très rapide.

C'est ici que la protection proactive intervient, grâce à la rapidité de ses réponses aux menaces nouvelles, ce qui augmente considérablement les chances de maintenir les ordinateurs fonctionnels et de les protéger contre les codes malveillants. C'est la raison pour laquelle BitDefender propose la technologie B-HAVE, qui analyse le comportement des codes potentiellement malveillants dans un environnement virtuel, élimine les faux positifs, et augmente significativement le taux de détection des codes nouveaux et inconnus.

C'est ainsi qu'une population de codes nouveaux ou mutés peut être anéantie en fonction de caractéristiques structurales ou comportementales, et non en utilisant une liste de menaces électroniques connues. Ceci présente l'avantage de réduire drastiquement le temps qui s'écoule entre mise en circulation du code malveillant et la diffusion de la mise à jour d'une signature anti-codes malveillants (connue également sous le nom de fenêtre d'exposition). Les tests indépendants effectués en janvier 2008 par Anti-Malware Test Lab ont déjà prouvé que la méthode heuristique B-HAVE de BitDefender détectait 63 % des menaces électroniques, sans avoir besoin d'une signature.[5]




[5] See "Testing of proactive antivirus protection: Key results from the proactive antivirus protection test", published 14 January 2008, in Anti-Malware Test Lab, http://www.anti-malwaretest.com/?q=node/39.

## Moteurs antispam intelligents

Dans la mesure où le spam réclame de plus en plus de vigilance, étant donné sa diversité et la rapidité de ses apparitions, les méthodes de détection doivent s'adapter à une réalité changeante. Les types de spam les plus complexes réclament des moteurs de détection plus intelligents. Pour mieux traiter le nouveau spam, les laboratoires BitDefender ont créé Neunet[6] (abréviation de neural network – réseau neuronal), un puissant filtre antispam. NeuNet est entraîné par le laboratoire BitDefender Antispam sur une série de messages spam pour apprendre à reconnaître le nouveau spam en comparant ses ressemblances avec les messages qu'il a déjà examinés. Les versions les plus récentes sont régulièrement adressées aux clients dans le cadre du processus courant de mise à jour.

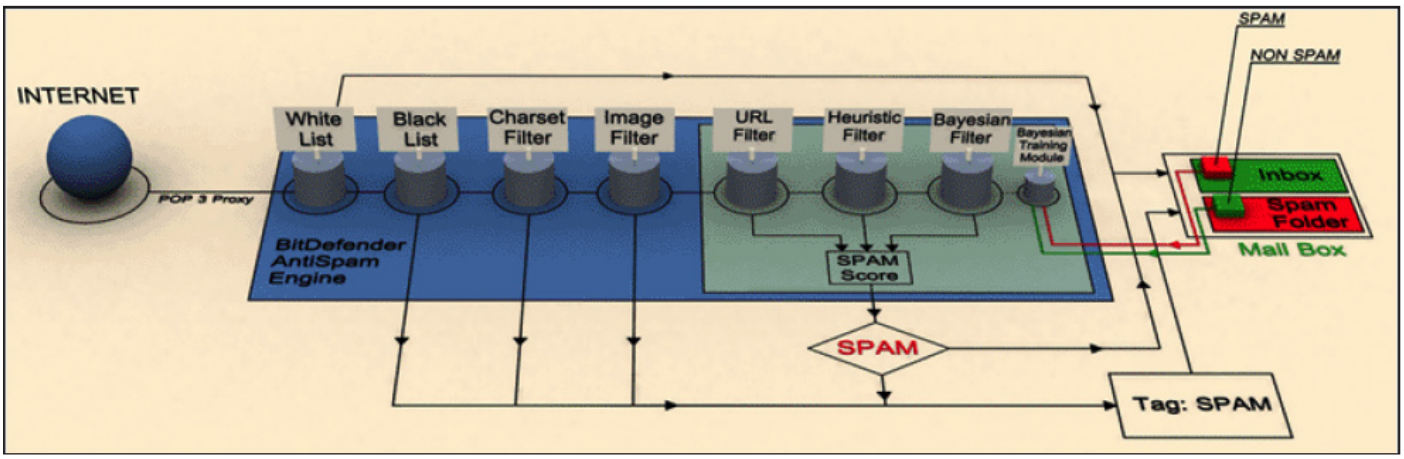
## Protection multiple

Connaître et appliquer tous les principes essentiels de la protection des serveurs de messagerie peut être utile, mais une recette n'est généralement réussie que grâce à l'ingrédient ajouté pour équilibrer les parfums. Concernant la protection des données cet ingrédient combine les technologies anti-codes malveillants et anti-spam. Voici les principaux outils que BitDefender met à la disposition des serveurs d'entreprises :

- Liste d'IP à autoriser/rejeter – bloque une liste d'adresses tout en autorisant des exceptions
- Liste noire des expéditeurs – filtrage global au niveau de la connexion
- Correspondance IP – pour empêcher l'utilisation de noms de domaines falsifiés
- Politiques antispam – permet de créer des politiques de groupes afin de définir différents niveaux de protection antispam
- Liste blanche – empêche les faux positifs
- Liste noire – empêche la réception de messages provenant de certaines adresses
- Filtre RBL – permet d'identifier le spam en fonction de la réputation du serveur de messagerie
- Filtre des polices de caractères – empêche la réception de courriers contenant certains caractères – Cyrillique etc.
- Filtre d'URL – bloque les liens vers des sites connus pour la diffusion de code malveillant
- Filtre bayésien – filtre antispam pouvant être entraîné et capable de discerner le courrier légitime du spam
- Anti-hameçonnage – protège contre les liens à double face qui dissimulent les tentatives de vol de données sensibles
- Protection contre le directory harvesting – empêche le vol d'adresses valides sur le serveur de messagerie.
- Protection antispyware – empêche le vol de données confidentielles et bloque l'installation d'applications non souhaitées

La figure ci-dessous résume l'ensemble du processus et indique les principaux composants que contient le filtre anti-spam de BitDefender :

[6] Pour une description complète du filtre NeuNet, veuillez consulter le document de présentation technique de Catalin Alexandru Cosoi "BitDefender Antispam NeuNet", disponible sur BitDefender, http://www.bitdefender.com/files/Main/file/BitDefender_Antispam_NeuNet.pdf.



Puisque que nous sommes dans le domaine de la gastronomie des serveurs de messagerie, n'oublions pas le sel ni le poivre ! Un produit de sécurité est aussi bon que ses mises à jour sont fréquentes et de qualité. S'appuyant sur un système avancé de mise à jour, les produits BitDefender pour serveurs de messagerie reçoivent les dernières mises à jour et correctifs, en fonction de quatre technologies configurables : à la demande, programmée, automatique et « pushed ». Les mises à jour « pushed » atteignent les serveurs clients à la seconde même où elles deviennent disponibles, sans attendre le moment de la prochaine mise à jour programmée, réduisant d'autant la menace que font peser les nouveaux virus.

Les correctifs et améliorations apportées au produit peuvent être téléchargées automatiquement et les administrateurs sont alertés de la sortie des nouvelles versions, ce qui leur permet de décider du moment de leur installation. De plus, les utilisateurs enregistrés bénéficient gratuitement de la mise à niveau du produit pendant la période de validité de la licence. Des prix spéciaux sont également proposés aux clients qui renouvellent leur licence.

## Education

Un principe d'hygiène de base reste que l'éducation sauve plus de vies que les antibiotiques. L'équivalent en ligne est également vrai : une des principales défenses contre de telles menaces reste l'éducation. Il n'existe pas d'efforts concertés dans ce domaine mais les entreprises et les états tournés vers l'avenir devraient reconnaître la nécessité d'éduquer les utilisateurs pour leur permettre de raisonner correctement sur la nature de la confiance, de l'identité et sur les technologies qu'ils utilisent quotidiennement. Si l'éducation en générale suppose un effort à long terme impliquant la société dans son ensemble, l'adoption d'un comportement raisonnablement prudent dans l'utilisation du courrier électronique dépend du sens des responsabilités de chaque individu. Appliquer quelques principes de sécurité en matière de messagerie, dictés par ce qui sont désormais des principes de bon sens en termes de sécurité des données, ne demande ni connaissances spécialisées ni beaucoup d'efforts. Voici quelques-uns de ces principes sur le mode OUI/NON :

- N'utilisez jamais les liens contenus dans les messages électroniques en provenance d'institutions financières, qui n'envoient jamais de mails non sollicités. Gardez présent à l'esprit qu'aucune institution financière ne vous demandera jamais par e-mail de données confidentielles, comme le code de votre carte bancaire par exemple.
- N'ouvrez les documents attachés que si vous connaissez l'expéditeur du courrier et avez confiance en lui, où dont vous êtes certain que leur contenu a été analysé. Ceci nécessite qu'une solution antivirus soit activée sur votre ordinateur. L'idéal étant que, en dehors de la sécurité du serveur de messagerie, une solution de sécurité soit installée sur votre ordinateur en tant que second rempart de protection contre les menaces Internet.
- Abstenez-vous d'indiquer votre adresse électronique dans les questionnaires fournis par diverses entreprises publicitaires car vous courez le risque de voir votre boîte de réception saturée par des courriers non sollicités. De même, si vous indiquez votre adresse sur un site Web, assurez-vous de le faire sous la forme nom@société.com pour éviter qu'elle ne soit interceptée par des propagateurs de spam.

## Conclusions

Les codes malveillants et le spam ne vont pas disparaître, mais ils peuvent être maîtrisés en recourant à tous les moyens disponibles, parmi lesquels l'éducation et l'utilisation de logiciels anti-spam et anti-virus. L'éducation en matière de sécurité des données dans ce contexte n'a pas besoin d'aller au-delà d'une sensibilisation aux conséquences de l'utilisation des adresses électroniques. La connaissance supplémentaire de l'existence des vecteurs d'attaques et des mécanismes qui les sous-tendent peut seulement augmenter leur sens du contrôle et de la sécurité quand ils utilisent Internet comme moyen de communication. Pour terminer, si l'utilisation d'une solution de sécurité électronique devient une pratique commerciale courante, au moins les éléments essentiels d'un certain équilibre auront été mis en place.