



MessageLabs Intelligence : Mai 2007

« Pics de spam – Le bélier du Spam »

Introduction

Ceci est l'édition de mai 2007 du rapport mensuel de MessageLabs Intelligence. Ce rapport fournit les dernières tendances de menaces et statistiques afin de vous informer de la lutte continue contre les virus, le spam et autres contenus indésirables.

Les résultats phares de ce rapport concernent :

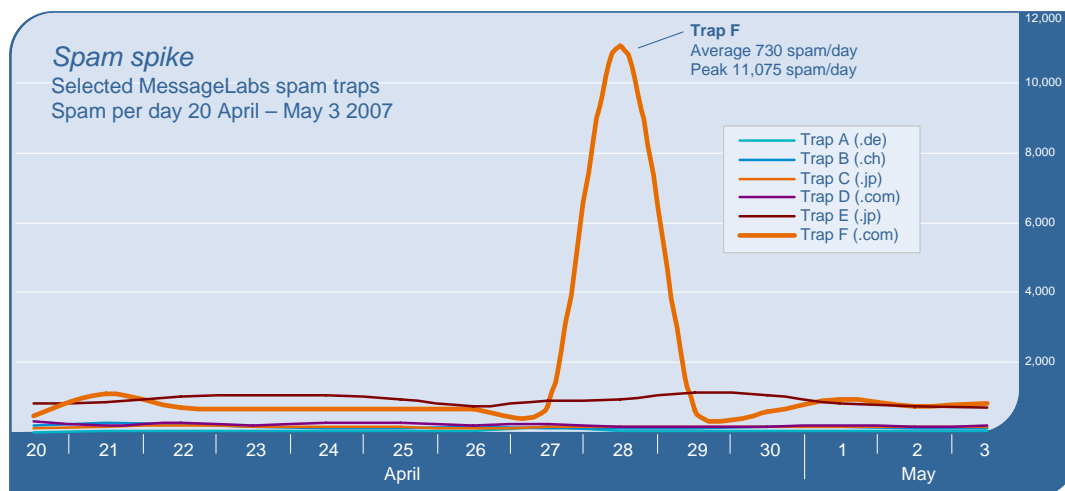
Spam – 72,7 % en mai (une baisse de 3,40 % depuis le mois d'avril)

Virus – Un mail sur 118,2 au mois de mai contenait un logiciel malveillant (une augmentation de 0,16 % depuis le mois d'avril)

Hameçonnage – Un mail sur 156,3 faisait partie d'une opération d'hameçonnage (une augmentation de 0,40 % depuis le mois d'avril)

Ce mois nous avons constaté une recrudescence d'une certaine activité de spam appelée pics, une technique de spam qui consiste à cibler des domaines individuels par des attaques particulièrement agressives. Le but d'un pic de spam est de mettre en échec les systèmes anti-spam résidents qui font largement appel aux signatures (plutôt qu'à des logiciels anti-virus de bureau). Pour les entreprises de petite taille, ce type d'attaque peut générer des problèmes sur les serveurs de messagerie de l'entreprise.

De la même façon qu'une attaque peut cibler les contre-mesures d'un anti-virus classique, un pic de spam peut déjà être terminé avant même que le fournisseur d'anti-spam n'ait eu le temps d'obtenir un échantillon et de produire une signature. L'exemple ci-dessous présente l'analyse d'un échantillon type de domaines de spams gérés par MessageLabs. Le pic a démarré entre 1h et 2h du matin et s'est achevé entre 2h et 3h de l'après-midi, soit une durée de 11 heures.

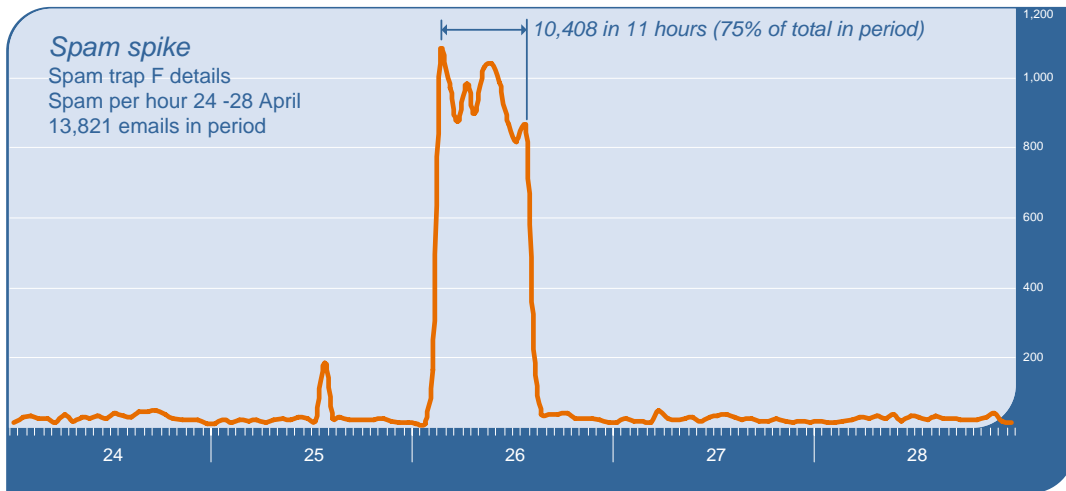




Sur le schéma, vous pouvez voir que les autres domaines gérés n'ont pas subi de pic à une telle échelle pendant le même intervalle de temps.



Si nous regardons de plus près le pic de spam ci-dessus, nous voyons que plus de 10 000 messages de spam ont été envoyés pendant cette période, représentant plus de 75 % du total des messages reçus par le domaine sur l'ensemble de la période.



Une autre technique intéressante de certains spammeurs consiste en une utilisation totalement différente d'images. Plutôt que d'intégrer une image dans le message lui-même, comme cela se fait traditionnellement, ces spammeurs enregistrent l'image sur plusieurs hébergeurs d'images différents, en général ceux qui ne nécessitent aucune inscription pour télécharger une image. Le lien vers l'image est inclus dans le corps du message, soit sous la forme d'un lien qui affiche le message lorsque l'on clique dessus, soit sous la forme d'une image HTML. En voici un exemple (certains éléments de l'adresse ont été enlevés pour des raisons de sécurité) :

```

```

Cette adresse permet d'afficher l'image suivante :



Le même groupe qui a lancé cette attaque a également abusé d'Imageshack, un site populaire d'hébergement d'images. Ce problème semble prendre de l'ampleur. Les hébergeurs trompés de cette façon ne prévoient aucun outil d'inscription ou même de différenciation permettant de contrôler que les images téléchargées proviennent bien d'une personne en chair et en os, et non d'un ordinateur. Un outil de différenciation est par exemple CAPTCHA, un test qui permet de distinguer une image téléchargée par une personne d'une image téléchargée automatiquement. De plus, les techniques



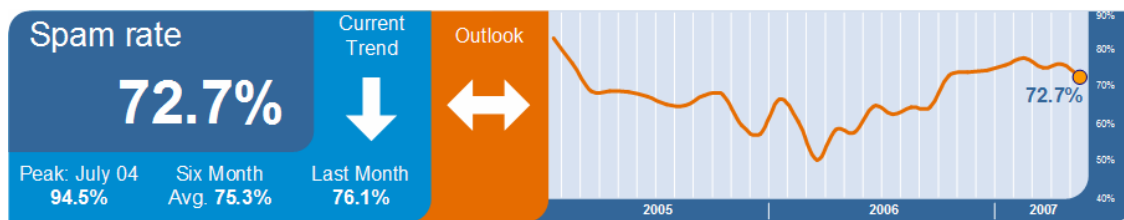
anti-spam classiques ont toujours autant de difficultés à protéger les utilisateurs de ce type de spam image.



Tendances globales et analyse de contenu

Les services anti-spam et anti-virus de MessageLabs se concentrent sur l'identification et la notification de messages indésirables issus de sources nuisibles nouvelles et inconnues et adressés à des destinataires valides.

Protection anti-spam Skeptic™ : En mai 2007, le ratio global de spam dans le trafic d'e-mail provenant de sources nuisibles nouvelles et inconnues, pour lesquelles les adresses des destinataires sont considérées comme valides, était de 72,7 % (1 sur 1,38), une baisse de 3,40 % par rapport au mois précédent.



Le chiffre de 72,7 % est en fait inférieur au « vrai » chiffre de spam puisque MessageLabs Traffic Management permet de contrôler la quantité de bande passante accordée à des sources nuisibles de spam *entièrement répertoriées*, et d' « étrangler » ces connexions en conséquence. Les connexions des spammeurs s'apparentent alors à celles d'un modem à très bas débit.

Elles rendent les essais d'envoi de spam aux clients de MessageLabs extrêmement pénibles, puisque Traffic Management repousse le spam vers les réseaux des spammeurs en ralentissant leur capacité d'envoi en masse. En conséquence, beaucoup de ces connexions finissent par dépasser le temps d'attente prévu ou passent à des cibles moins protégées. Si nous considérons le nombre total des spams qui arrivent sur les pots de miels de MessageLabs, qui, comparativement, ne sont pas protégés, ce chiffre sera bien plus près de 85,3 %, soit une augmentation de 1,7 % depuis le mois d'avril. Ceci est largement dû aux contrôles de Traffic Management, qui sont capables d'identifier et de stopper une plus grande quantité de spam connu provenant de sources malveillantes connues. La quantité de spam nouveau et précédemment inconnu a baissé de 76,1 % à 72,7 % au mois de mai. Pour plus d'information, veuillez vous reporter au paragraphe sur le Traffic Management du présent rapport.

Le spam image a été largement abordé récemment. Certains pensent que ces spams images représentent la majorité du spam actuellement en circulation. D'autres, comme MessageLabs, estiment ce pourcentage à 15 à 20 % du total de spam. L'image est souvent créée au vol, en utilisant des modèles spécialisés et des moteurs de spam contrôlés par un botnet comme Rustock. Le spam image peut également être envoyé sous la forme de texte, comme cela se fait si souvent. Tout dépend donc de la proportion que représente le spam image dans l'échantillon au moment où celui-ci est analysé. Le même échantillon peut produire des résultats différents à différents moments. Un des derniers rebondissements dans la problématique du spam image est que l'image contenue dans le message de spam peut être hébergée sur un ou plusieurs hébergeurs gratuits qui ne nécessitent aucune identification pour pouvoir télécharger une image.

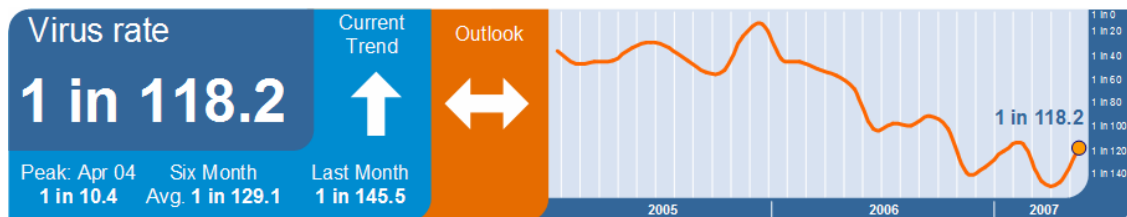
Ces messages sont uniquement envoyés pendant les périodes de week-end et ne contiennent aucun lien ou image intégrée, mais l'image reste visible si l'utilisateur souhaite la voir. Certains de ces sites sont plus prudents face à ces abus et sont capables de supprimer ces images assez rapidement, mais d'autres moins. Ce spam image est invariablement lié à des messages à fausses informations boursières. Dans la dernière campagne de spam, le même groupe réutilisait certaines images. Sur une période d'une heure, 963 liens Freeshare.us ont été identifiés. Sur ceux-ci, 156 étaient uniques,



certaines images étant utilisées entre 15 et 25 fois. Même situation avec Insepix.com. Huit cent dix-sept liens ont été identifiés sur une période d'une heure. Sur ceux-ci, 163 étaient uniques, les mêmes images étant utilisées entre 10 et 20 fois.

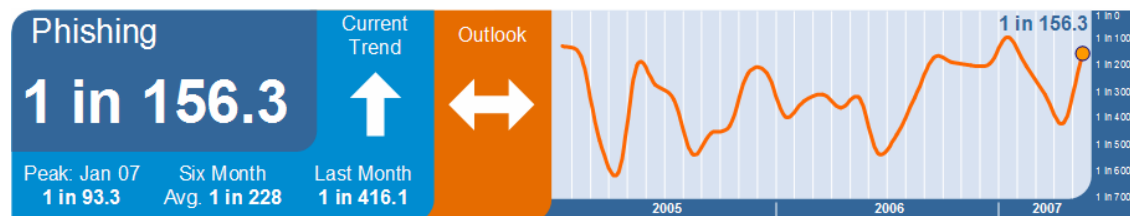


Protection anti-virus et anti-cheval de Troie Skeptic™ : Le ratio global de virus transmis par e-mail dans le flot de messages, provenant de sources nuisibles nouvelles et jusque-là inconnues et destiné à des destinataires valides était de 1 pour 118,2 (0,85 %) en mai, soit une baisse de 0,16 % par rapport au mois dernier.



En poursuivant l'action du mois dernier, MessageLabs a de nouveau analysé les attaques ciblées très spécialisées interceptées au mois d'avril. MessageLabs a en tout arrêté 595 e-mails dans 180 domaines différents pour 168 clients. Bien que les chiffres soient légèrement inférieurs au mois dernier, 64 % des attaques ont exploité les vulnérabilités de Microsoft Word, 17 % celles de Microsoft Excel et 14 % celles de Microsoft PowerPoint. Le mois dernier, PowerPoint était le principal vecteur d'attaque, mais il a été dépassé par Word. Pour éviter la détection par les logiciels anti-virus classiques, la majorité des attaques est composée d'un e-mail destiné à un individu.

Hameçonnage : Le mois de mai a montré une hausse de 0,40 % de la proportion d'attaques d'hameçonnage par comparaison au mois précédent. Un e-mail sur 156,3 (0,64 %) était une forme ou l'autre d'hameçonnage.



En considérant le nombre d'attaques d'hameçonnage par e-mail comme une partie des menaces transmises par e-mail au même titre que les virus et les chevaux de Troie, ce nombre d'attaques a également baissé de 43,9 % et représente désormais 78,9 % de tous les e-mails malveillants interceptés par MessageLabs en mai, le nombre le plus important depuis décembre 2006.

L'analyse des botnets derrière un grand nombre des dernières attaques d'hameçonnage révèle certains faits intéressants. Par exemple, la taille du botnet utilisé pour mener la plus grosse attaque d'hameçonnage pendant le mois de mai comprenait environ 500 robots. Ce même botnet était capable de générer près de 225 000 e-mails d'hameçonnage pour une seule cible, tout en étant responsable de la distribution de 55 souches différentes de près de 10 000 virus.



Skeptic™ Web Security Services Version 2.0 : MessageLabs Web Security Services version 2.0, conçue sur la propre technologie de MessageLabs grâce à Skeptic, permet à MessageLabs de récupérer les dernières informations relatives aux menaces et aux réputations à partir d'autres protocoles, comme les e-mails, et d'appliquer ces connaissances au trafic Internet.

Web Security Services (Version 2.0) Activity:

| Policy-Based Filtering | | Web Viruses and Trojans | | Potentially Unwanted Programs | |
|-------------------------|--------|-----------------------------------|--------|-------------------------------|--------|
| Advertisements & Popups | 61.40% | Trojan-Downloader.Win32.IstBar.pk | 60.38% | Adware-SaveNow | 50.89% |
| Personals & Dating | 5.68% | Exploit-ANIfile.c | 3.95% | Adware-GAIN | 42.55% |
| Adult/Sexually Explicit | 4.18% | JS/Downloader-AUD | 3.82% | Adware-ISTbar.b | 5.86% |
| Photo Searches | 4.04% | VBS/Psyme | 3.38% | Adware-HotBar | 0.31% |
| Streaming Media | 3.83% | Exploit.HTML.Mht | 2.19% | Adware-MediaTickets | 0.09% |
| Spyware | 3.82% | JS/Wonka | 1.85% | Adware-ZangoSA | 0.07% |
| Chat | 2.95% | Suspicious IFrame.b | 1.82% | Adware-HotBar.dr | 0.05% |
| Shopping | 2.69% | Trojan-Downloader.VBS.Small.co | 1.67% | AdwareDropper-I.gen | 0.05% |
| Gambling | 1.89% | ObfuscatedHtml | 1.51% | Adware-Softomate | 0.03% |
| Unclassified | 1.39% | Exploit.JS.ADODB.Stream.y | 1.28% | Adware-IstBar.dldr | 0.02% |

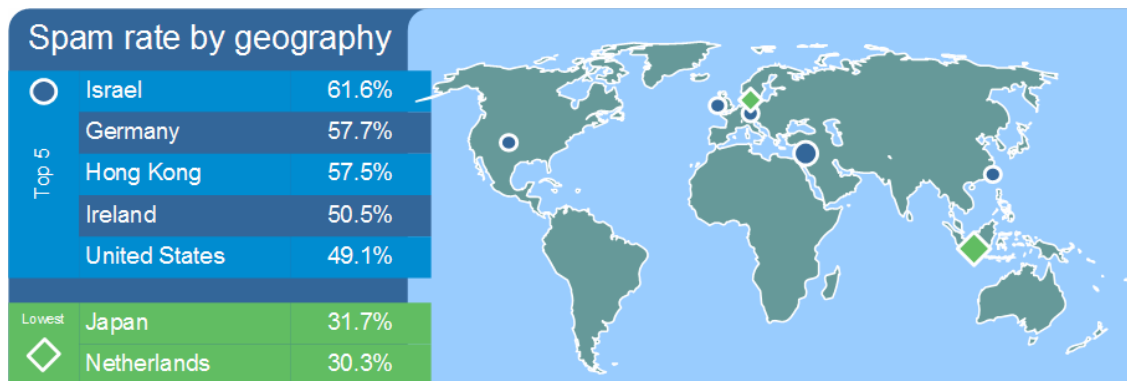
Dans le tableau ci-dessus, on constate que les Publicités et Fenêtres publicitaires (61,40 %) sont les déclencheurs les plus courants de filtrage basé sur des règles, tel qu'appliqué par MessageLabs pour ses clients. Ceci représente une augmentation de 5,64 % par rapport au mois précédent. Une analyse plus poussée montre que 9,11 % des logiciels malveillants interceptés en mai étaient nouveaux.

La catégorie « Non-classé » identifie de nouveaux sites non catalogués précédemment, qui peuvent nécessiter d'être interdits. La catégorie « Non-classé » est plus fiable lorsque de nouvelles règles sont définies. Autrement dit, de nouveaux sites malveillants récemment détectés peuvent être traités de façon plus appropriée jusqu'à leur classification, offrant ainsi une protection contre des sites à domaine jetable qui peuvent apparaître et disparaître dans un délai de 24 à 48 heures. Ces sites peuvent être utilisés à des fins peu honorables, comme les sites hébergeant du spam et du hameçonnage, des chevaux de Troie voleurs d'information et d'autres activités frauduleuses. 89,52 % des virus d'Internet et 82,57 % des logiciels espions interceptés ont été classés dans cette catégorie, ce qui signifierait que la plupart de ces interceptions ont été hébergées sur des sites Internet jusque-là inconnus et non classés.

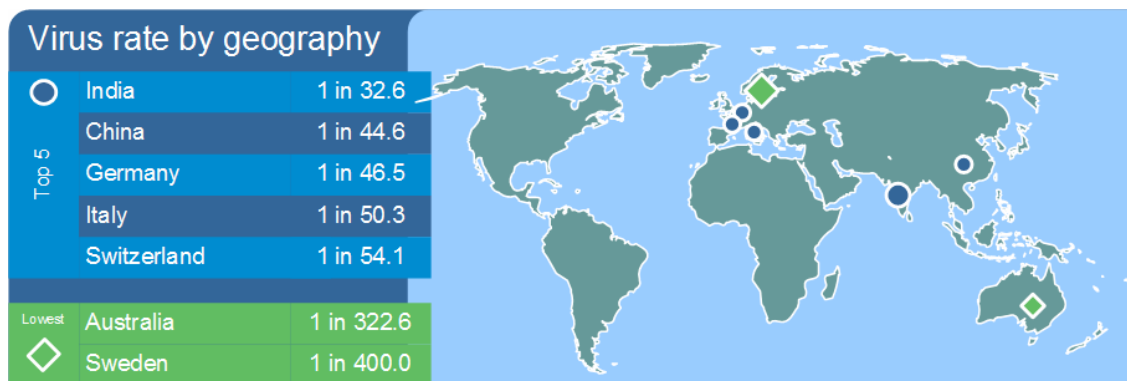


Analyse géographique : basée sur les pays ciblés

Analyse mensuelle : En analysant, lorsque c'est possible, la répartition géographique du trafic des e-mails, MessageLabs compile des données illustrant les taux d'impact et de vulnérabilité du spam et des virus propres aux zones géographiques. Les tableaux suivants représentent l'impact et les ratios pour mai 2007.



Les niveaux de spam en Israël, en dépit d'une baisse de 11,7 % depuis le mois d'avril, ont transformé cette zone géographique en cible majoritaire. Les niveaux ont baissé pour tous les pays listés dans le tableau ce mois-ci.



Malgré une chute de 0,09 % , l'Inde reste la région la plus touchée ce mois-ci. La plus forte hausse a été notée en Chine, où les niveaux ont augmenté de 1,07 % en mai, la plaçant ainsi en seconde position dans le tableau.

Vous trouverez plus de détails dans les annexes à la fin de ce rapport.

Analyse par secteur d'activité

Analyse mensuelle : En analysant, lorsque c'est possible, la répartition sur le marché du trafic des messages, MessageLabs compile les données illustrant les taux d'impact et de vulnérabilité du spam et des virus propres aux principaux secteurs. Les tableaux suivants représentent les impacts et les ratios pour mai 2007.

| Spam rate by vertical | | | Virus rate by vertical | | |
|-----------------------|---------------|-------|------------------------|---------------|------------|
| Top 5 | Agriculture | 63.1% | Top 5 | Chem/Pharm | 1 in 64.9 |
| | Manufacturing | 55.3% | | Education | 1 in 72.5 |
| | Education | 52.5% | | Wholesale | 1 in 80.6 |
| | IT Services | 50.6% | | Manufacturing | 1 in 93.5 |
| | Wholesale | 49.9% | | Retail | 1 in 97.1 |
| Lowest | Building/Cons | 31.6% | Lowest | Agriculture | 1 in 384.6 |
| | Finance | 27.3% | | Telecoms | 1 in 476.2 |

La seule hausse des niveaux de spam tous secteurs industriels confondus au mois de mai a été observée dans le domaine de l'agriculture, secteur pour lequel le niveau a augmenté de 8,1 % depuis le mois d'avril. La baisse la plus importante a été notée pour le secteur BTP, qui a atteint 11,1 %.

La plus forte augmentation d'activité virale au cours du mois de mai s'est produite dans le secteur chimique et pharmaceutique, où les niveaux ont augmenté de 0,65 % depuis le mois d'avril. La plus forte baisse concernait le secteur des services aux entreprises.

Vous trouverez plus de détails dans les annexes à la fin de ce rapport.



Gestion du trafic (niveau de protocole)

La gestion du trafic permet de réduire encore le volume global de messages par le biais de techniques opérant au niveau du protocole. Les expéditeurs indésirables sont identifiés et les connexions au serveur de messagerie sont ralenties à l'aide de fonctionnalités intégrées dans le protocole TCP. Les volumes entrants de spam identifié sont considérablement ralentis, alors que les messages légitimes sont expédiés.

En mai, MessageLabs a traité plus de 2,57 milliards de connexions SMTP par jour, dont 88,7 % ont été « étranglées » sous l'effet de contrôles de protocole de gestion de trafic portant sur des messages manifestement indésirables ou malveillants. Les autres connexions ont ensuite été traitées par les contrôles de gestion des connexions de MessageLabs et Skeptic™.

Gestion des connexions

La gestion des connexions est particulièrement efficace pour stopper les attaques de récolte de répertoires, les attaques en force et les attaques de déni de service concernant les messageries électroniques lorsque des expéditeurs indésirables envoient de gros volumes de messages pour forcer l'accès du spam ou perturber les communications. La gestion des connexions intervient au niveau SMTP à l'aide de techniques de contrôle des connexions légitimes au serveur de messagerie. Elle comprend les éléments suivants:

Validation SMTP : identifie les messages indésirables issus de sources de spam et de virus connues, la source étant alors identifiée sans équivoque comme étant un proxy ouvert ou un botnet, et rejette la connexion en conséquence. En mai, une moyenne de 43,7 % de messages entrants a été interceptée en provenance de botnets et autres sources nuisibles connues et rejetée en conséquence.

Validation utilisateur : réduit le volume global de messages pour les domaines enregistrés en rejetant les connexions pour lesquelles le destinataire est identifié comme étant non valide ou inexistant. En mai, une moyenne de 4,8 % d'adresses de destinataires a été identifiée comme n'étant pas valide. Il s'agissait de tentatives d'attaque de répertoires par le biais de domaines, qui ont ainsi pu être protégées contre des attaques.

En résumé

Le tableau ci-dessous détaille l'impact actuel du trafic et des techniques de gestion des connexions sur le volume de messages indésirables mesuré par MessageLabs Intelligence. Sans ces couches multiples de défense supplémentaires, le trafic de spam destiné aux clients de MessageLabs en mai aurait atteint près de 85,3 % du trafic global des e-mails, une hausse de 1,7 % par rapport au mois précédent.

| Zone | Traffic Management (contrôle de protocole) | SMTP Validation (analyse de comportement) | Validation utilisateur (attaques de répertoires) |
|----------------|---|--|---|
| États-Unis | 91.4% | 50.3% | 3.6% |
| Royaume-Uni | 82.1% | 35.2% | 4.2% |
| Europe | 76.4% | 35.9% | 8.4% |
| Asie-Pacifique | 22.4% | 38.4% | 1.1% |
| Monde | 88.7% | 43.7% | 4.8% |

Impact des techniques de gestion de connexion

MessageLabs est le principal fournisseur mondial de services de sécurité sur Internet et de messagerie intégrée, avec plus de 15 000 clients allant de petites entreprises aux 500 de la revue Fortune, localisées dans plus de 80 pays. MessageLabs fournit toute une gamme de services de gestion de sécurité de protection, de contrôle, de cryptage et de communication d'archives via les e-mails, Internet et les messageries instantanées.



Ces services sont fournis par l'infrastructure globalement distribuée de MessageLabs et sont assistés d'experts sécurités 24h sur 24. Ceci fournit une solution pratique et rentable pour gérer et réduire les risques tout en fournissant une certitude dans les échanges d'informations commerciales. Pour plus d'informations, veuillez visiter le site www.messagelabs.com.

Pour de plus amples informations sur MessageLabs Intelligence, visitez notre site www.messagelabs.com/intelligence et abonnez-vous pour recevoir régulièrement des alertes et des rapports.

Note : Tous les chiffres mentionnés dans le présent rapport étaient exacts au moment de la mise sous presse.



Annexes

Annexe I : Pourcentage de spam par région (mai 2007)

| | May | April | Change |
|----------------------|-------|-------|--------|
| Australia | 33.4% | 40.0% | -6.6% |
| Austria | 42.9% | 51.4% | -8.5% |
| Belgium | 43.8% | 48.5% | -4.7% |
| Canada | 43.8% | 53.6% | -9.8% |
| China | 36.6% | 41.5% | 4.9% |
| France | 48.3% | 56.2% | -7.9% |
| Germany | 57.7% | 66.3% | -8.6% |
| Hong Kong | 57.5% | 63.7% | -6.2% |
| India | 35.3% | 44.4% | -9.1% |
| Ireland | 50.5% | 59.1% | -8.6% |
| Israel | 61.6% | 73.3% | -11.7% |
| Italy | 39.9% | 48.0% | -8.1% |
| Japan | 31.7% | 38.8% | -7.1% |
| Netherlands | 30.3% | 39.8% | -9.5% |
| Singapore | 40.6% | 31.2% | 9.4% |
| Spain | 40.0% | 51.0% | -11.0% |
| Sweden | 32.3% | 48.6% | -16.3% |
| Switzerland | 42.2% | 46.6% | -4.4% |
| United Arab Emirates | 41.8% | 45.3% | -3.5% |
| United Kingdom | 40.7% | 47.5% | -6.8% |
| United States | 49.1% | 55.9% | -6.8% |



Annexe II : Pourcentage de virus par région (mai 2007)

| | May | April | Change |
|----------------------|-------|-------|--------|
| Australia | 0.31% | 0.41% | -0.10% |
| Austria | 1.44% | 0.99% | 0.45% |
| Belgium | 0.37% | 0.30% | 0.07% |
| Canada | 0.70% | 0.57% | 0.13% |
| China | 2.24% | 1.17% | 1.07% |
| France | 1.44% | 1.29% | 0.15% |
| Germany | 2.15% | 1.63% | 0.52% |
| Hong Kong | 1.63% | 1.03% | 0.60% |
| India | 3.07% | 3.16% | -0.09% |
| Ireland | 1.06% | 2.05% | -0.99% |
| Israel | 1.14% | 0.72% | 0.42% |
| Italy | 1.99% | 1.38% | 0.61% |
| Japan | 0.47% | 0.59% | -0.12% |
| Netherlands | 0.38% | 0.34% | 0.04% |
| Singapore | 1.40% | 1.20% | 0.20% |
| Spain | 1.26% | 1.02% | 0.24% |
| Sweden | 0.25% | 0.15% | 0.10% |
| Switzerland | 1.85% | 1.20% | 0.65% |
| United Arab Emirates | 1.77% | 1.12% | 0.65% |
| United Kingdom | 0.76% | 0.67% | 0.09% |
| United States | 0.88% | 0.70% | 0.18% |



Annexe III : Pourcentage de virus par secteur (mai 2007)

| | May | April | Change |
|---------------------------|-------|-------|--------|
| Accom/Catering | 37.7% | 45.1% | -7.4% |
| Agriculture | 63.1% | 55.0% | 8.1% |
| Building/Cons | 31.6% | 42.7% | -11.1% |
| Business Support Services | 46.8% | 57.5% | -10.7% |
| Chem/Pharm | 44.2% | 52.1% | -7.9% |
| Education | 52.5% | 61.3% | -8.8% |
| Estate Agents | 34.2% | 41.0% | -6.8% |
| Finance | 27.3% | 35.1% | -7.8% |
| General Services | 37.3% | 44.0% | -6.7% |
| Gov/Public Sector | 37.9% | 40.1% | -2.2% |
| Health Care | 46.0% | 52.6% | -6.6% |
| IT Services | 50.6% | 56.1% | -5.5% |
| Manufacturing | 55.3% | 62.1% | -6.8% |
| Marketing/Media | 49.3% | 55.5% | -6.2% |
| Mineral/Fuel | 44.5% | 48.9% | -4.4% |
| Non-Profit | 40.5% | 45.0% | -4.5% |
| Prof Services | 41.0% | 49.8% | -8.8% |
| Recreation | 38.7% | 44.4% | -5.7% |
| Retail | 44.0% | 50.6% | -6.6% |
| Telecoms | 40.2% | 47.5% | -7.3% |
| Transport/Util | 46.8% | 52.6% | -5.8% |
| Wholesale | 49.9% | 57.6% | -7.7% |



Annexe IV : Pourcentage de virus par secteur (mai 2007)

| | May | April | Change |
|---------------------------|-------|-------|--------|
| Accom/Catering | 0.66% | 0.44% | 0.22% |
| Agriculture | 0.26% | 0.41% | -0.15% |
| Building/Cons | 0.52% | 0.46% | 0.06% |
| Business Support Services | 0.29% | 1.29% | -1.00% |
| Chem/Pharm | 1.54% | 0.89% | 0.65% |
| Education | 1.38% | 1.66% | -0.28% |
| Estate Agents | 0.89% | 0.52% | 0.37% |
| Finance | 0.53% | 0.54% | -0.01% |
| General Services | 0.68% | 0.56% | 0.12% |
| Gov/Public Sector | 0.70% | 0.72% | -0.02% |
| Health Care | 0.63% | 0.64% | -0.01% |
| IT Services | 0.89% | 0.79% | 0.10% |
| Manufacturing | 1.07% | 0.79% | 0.28% |
| Marketing/Media | 0.92% | 0.80% | 0.12% |
| Mineral/Fuel | 0.67% | 0.54% | 0.13% |
| Non-Profit | 0.69% | 0.58% | 0.11% |
| Prof Services | 0.91% | 0.75% | 0.16% |
| Recreation | 0.89% | 0.59% | 0.30% |
| Retail | 1.03% | 1.21% | -0.18% |
| Telecoms | 0.21% | 0.19% | 0.02% |
| Transport/Util | 0.57% | 0.40% | 0.17% |
| Wholesale | 1.24% | 0.87% | 0.37% |