



## MessageLabs Intelligence : Juillet 2007

### « Le spam PDF en augmentation »

#### Introduction

Ceci est l'édition de juillet 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.

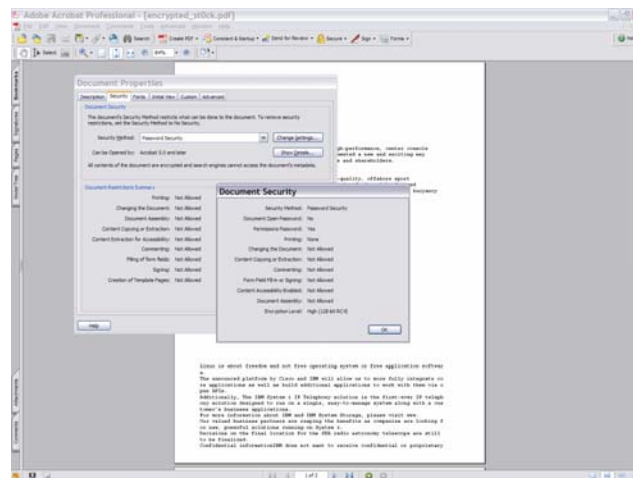
Les résultats phares de ce rapport concernent :

*Spam – 71,0 % en juillet (une baisse de 1,40 % depuis le mois de juin)*

*Virus – Un mail sur 72,4 au mois de juillet contenait un logiciel malveillant (une augmentation de 0,59 % depuis le mois de juin)*

*Hameçonnage – Un mail sur 111,8 faisait partie d'une opération de hameçonnage (une augmentation de 0,09 % depuis le mois de juin)*

Suite au rapport de MessageLabs Intelligence de juin 2007, dans lequel nous analysons la tendance à l'utilisation de pièces jointes PDF au sein de messages de spam financier, MessageLabs a constaté ce mois l'adoption de cette approche par d'autres polluposteurs. Augmentant en complexité, certains des derniers exemples montrent comment les documents PDF sont générés automatiquement, avec les paramètres de protection de document activés. Les polluposteurs utilisent le modèle de sécurité PDF pour interdire l'impression, la copie de texte dans le presse-papiers, etc. Par exemple :



Cette tactique est déployée dans l'espoir de rendre difficile l'analyse et l'identification du contenu du message par les contre-mesures anti-spam traditionnelles. Avec ces caractéristique de « sécurité » activées, les e-mails sont davantage susceptibles de contourner les moyens de détection classiques. Le PDF contient toujours le « Poison de Bayes », l'inclusion de longues listes de mots aléatoires à la fin du document, visant à dissimuler la vraie nature du message spam pendant toute analyse anti-spam



traditionnelle. Environ 20 % de tous les spams d'image sont désormais sous format PDF. Le taux varie chaque minute en fonction de l'attention que les polluposteurs accordent à cette technique.

Les polluposteurs par PDF se classent globalement en deux catégories :

**Simples/Amateurs** : Ces polluposteurs élaborent des documents PDF à l'aide d'outils ordinaires tels que MS Word et utilisent le même PDF pour tous leurs envois de spams.

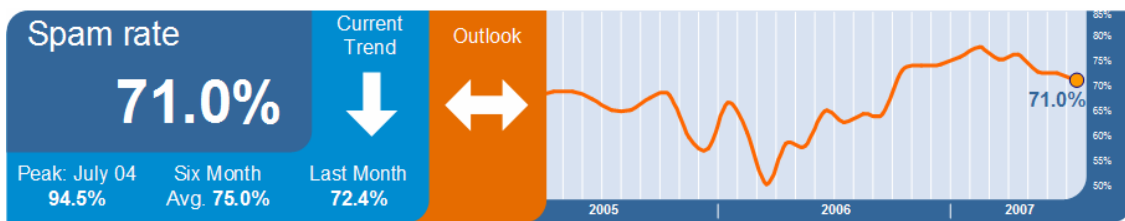
**Professionnels** : Il s'agit ici de polluposteurs plus expérimentés qui joignent un PDF différent dans chaque message de spam. Les PDF sont répartis au hasard et ne contiennent généralement pas de texte. Ces polluposteurs intègrent plutôt des images réparties au hasard dans les documents PDF et utilisent également d'autres tactiques telles que les tailles de page aléatoires.



### 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.

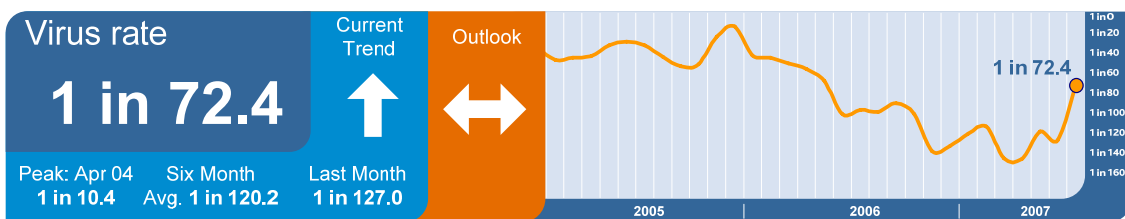
**Protection anti-spam Skeptic™** : En juillet 2007, le ratio global de spam dans le trafic d'e-mail provenant de sources nuisibles nouvelles et inconnues, pour lesquelles les adresses des destinataires sont considérées comme valides était de 71,0 % (1 sur 1,38), une baisse de 1,4 % par rapport au mois précédent.



Le ratio de 71,0 % est en fait inférieur au « vrai » ratio du spam puisque MessageLabs Traffic Management permet de contrôler la quantité de bande passante donnée aux sources nuisibles de spam *entièrement répertoriées* et réduit ces connexions, en les ralentissant. Pour les polluposteurs, elles paraissent comme des liaisons avec un modem à très bas débit.

Ceci a rendu les essais d'envoi de spam aux clients de MessageLabs par les polluposteurs incroyablement difficiles, puisque Traffic Management repousse le spam vers les réseaux des polluposteurs en ralentissant leur capacité à les envoyer en masse. En fait, beaucoup de ces connexions sont en « time-out » ou passent sur 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 83,4 %, une augmentation de 2,4 % depuis le mois de juin. Les contrôles de Traffic Management en sont la cause principale, qui peuvent identifier et arrêter une grande part du spam connu en provenance de sources malveillantes. La proportion de spam nouveau et jusque-là inconnu est passée de 72,4 % à 71 % en juillet. Pour plus d'information, veuillez vous reporter au paragraphe sur le Traffic Management du présent rapport.

**Protection anti-virus et anti-cheval de Troie Skeptic™** : Le ratio global de virus transmis par e-mail, présent dans le flot de messages, provenant de sources nuisibles nouvelles et jusque-là inconnues et destiné à des destinataires valides, était de 1 pour 72,4 (1,38 %) en juillet, soit une augmentation de 0,59 % par rapport au mois dernier.





**Hameçonnage :** Le mois de juillet a vu une augmentation de 0,09 % de la proportion d'attaques de hameçonnage par rapport au mois précédent. Un e-mail sur 111,8 (0,89 %) était une attaque de hameçonnage.



Si l'on considère le nombre d'attaques de 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 7,8 % depuis le mois précédent et représente désormais 64,8 % de tous les e-mails malveillants interceptés en juillet.

**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 49.34%	Suspicious IFrame.b 19.35%	PUP-GAIN 63.06%
Streaming Media 9.94%	VBS/Psyme 9.05%	PUP-SaveNow 36.32%
Personals & Dating 8.50%	JS/Downloader-AUD 4.60%	PUP-HotBar 0.23%
Gambling 6.99%	Trojan-Downloader.Win32.Agent.bls 4.15%	PUP-ZangoSA 0.19%
Downloads 4.48%	Trojan-Downloader.JS.Agent.kd 4.07%	PUP-ISTBar 0.05%
Adult/Sexually Explicit 4.01%	New Malware.n 4.00%	PUPDropper-I.gen 0.03%
Photo Searches 3.22%	Exploit-ANIfile.c 3.55%	PUP-WebHancer 0.03%
Spyware 2.03%	Trojan-Downloader.VBS.Small.co 2.90%	PUP-HotBar.dr 0.03%
Unclassified 1.58%	Trojan-Downloader.JS.Psyme.hz 2.26%	PUP-SpyStormer 0.02%
Chat 1.46%	Tool-TFTPD32 2.26%	PUP-DFC 0.02%

Dans le tableau ci-dessus, on constate que les Publicités et Fenêtres publicitaires (49,34 %) sont les déclencheurs les plus courants du filtrage basé sur des règles appliqué par MessageLabs pour ses clients. Ceci représente une baisse de 0,31 % par rapport au mois précédent. Une analyse plus poussée montre que 28,30 % des logiciels malveillants interceptés en juillet étaient nouveaux.

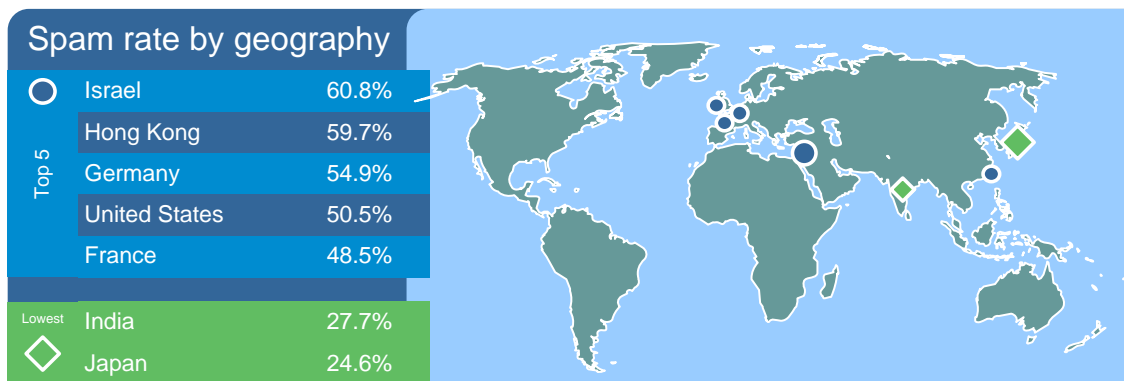
La catégorie « Non-classé » identifie de nouveaux sites non catalogués précédemment, qui peuvent nécessiter une interdiction. La catégorie « Non-classé » est plus fiable lorsque de nouvelles règles sont définies. Cela signifie que de nouveaux sites malveillants récemment détectés peuvent être traités 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.

89,60 % des virus d'Internet et 61,64 % des logiciels espions interceptés ont été classés dans la catégorie Non-classé, ce qui signifierait que la plupart de ces interceptions ont été hébergées sur des sites Internet jusque-là inconnus et non classés. Chaque jour, 989 nouveaux sites malveillants ont en moyenne été identifiés et bloqués en juillet.

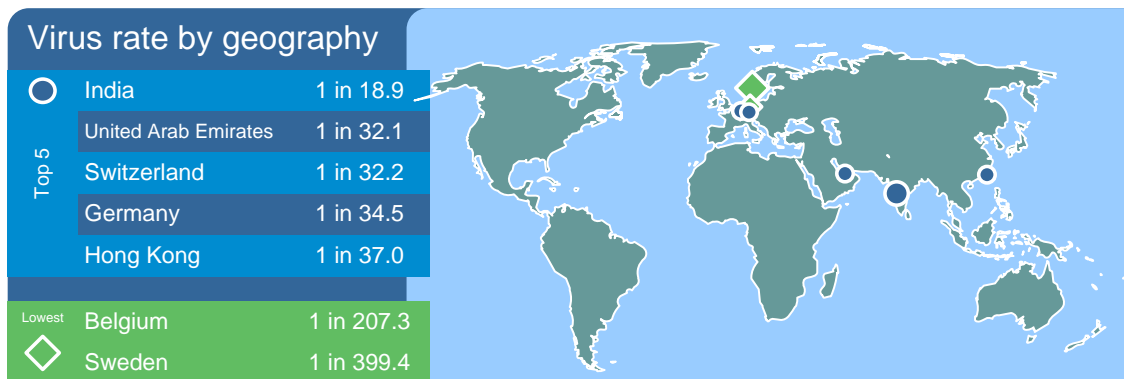


### Analyse géographique : basée sur les pays ciblés

**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 donnent un reflet des impacts et des ratios pour juillet 2007 :



Les niveaux de spam en Israël sont restés stables pour le second mois consécutif, avec 60,8 % de tout le trafic d'e-mail, faisant du pays la zone géographique la plus ciblée ce mois-ci. L'augmentation la plus importante des niveaux de spam concerne la Chine avec 18,3 %, suivie des États-Unis avec 5,9 %.



L'Inde reste la zone la plus affectée ce mois-ci avec une augmentation de 2,08 %, représentant la plus forte hausse de tous les pays en juillet. Les niveaux de virus ont diminué en Suède de 0,03 %, le seul pays à connaître une baisse de l'activité malveillante en juillet.

Des détails supplémentaires sont fournis en annexe, 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 donnent un reflet des impacts et des ratios pour juillet 2007 :

Spam rate by vertical			Virus rate by vertical		
Top 5	Agriculture	66.8%	Chem/Pharm	1 in 37.0	
	Manufacturing	57.1%	Education	1 in 39.6	
	Education	53.8%	Retail	1 in 51.2	
	Marketing/Media	50.9%	Prof Services	1 in 58.7	
	Health Care	49.1%	Wholesale	1 in 61.7	
Lowest	Building/Cons	31.6%	Agriculture	1 in 302.5	
	Finance	29.3%	Telecoms	1 in 348.4	

Le secteur caritatif a subi la plus forte augmentation de l'activité de spam parmi tous les secteurs en juillet, avec une hausse de 10,3 % par rapport au mois de juin, et se place en huitième position des secteurs les plus ciblés par le spam. Les cinq premiers secteurs ont tous subi une augmentation du spam entre 1,4 % et 4,6 %. La plus forte baisse concerne le secteur des transports (3,6%).

La plus forte hausse de l'activité virale en juillet frappe le secteur de l'éducation, où les niveaux ont augmenté de 1,78 % par rapport au mois de juin. La seule baisse enregistrée concerne le secteur financier, où les niveaux ont diminué de 0,29 %.

Des détails supplémentaires sont fournis en annexe, 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 juillet, MessageLabs a traité une moyenne de 1,76 milliard de connexions SMTP par jour, à un rythme de 1,3 message par connexion, dont 87,7 % ont été ralenties par des contrôles de protocole de gestion de trafic identifiant, sans équivoque possible, les contenus 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 juillet, une moyenne de 45,2 % de messages entrants a été interceptée en provenance de botnets et autres sources nuisibles connues et rejetés 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 juillet, une moyenne de 4,6 % 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 protégés 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 juillet aurait atteint près de 83,4 % du trafic global des e-mails, une hausse de 2,4 % par rapport au mois précédent.

Zone	Traffic Management (contrôle de protocole)	SMTP Validation (analyse de comportement)	Validation utilisateur (attaques de répertoires)
États-Unis	90.2%	45.2%	4.4%
Royaume-Uni	67.8%	67.8%	3.4%
Europe	78.2%	39.1%	6.4%
Asie-Pacifique	52.8%	44.2%	1.1%
<b>Monde</b>	<b>87.7%</b>	<b>45.2%</b>	<b>4.6%</b>

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](http://www.messagelabs.com).

Pour de plus amples informations sur MessageLabs Intelligence, visitez notre site [www.messagelabs.com/intelligence](http://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 (juillet 2007)**

	July	June	Change
Australia	33.1%	35.5%	-2.4%
Austria	42.1%	46.2%	-4.1%
Belgium	42.9%	42.9%	0.0%
Canada	41.4%	40.3%	1.1%
China	49.8%	31.5%	18.3%
France	48.5%	49.5%	-1.0%
Germany	54.9%	57.6%	-2.7%
Hong Kong	59.7%	58.0%	1.7%
India	27.7%	27.0%	0.7%
Ireland	45.0%	51.3%	-6.3%
Israel	60.8%	60.8%	0.0%
Italy	30.8%	35.9%	-5.1%
Japan	24.6%	26.8%	-2.2%
Netherlands	32.4%	31.4%	1.0%
Singapore	37.7%	36.6%	1.1%
Spain	32.1%	35.1%	-3.0%
Sweden	30.4%	30.9%	-0.5%
Switzerland	37.9%	40.7%	-2.8%
United Arab Emirates	35.2%	39.3%	-4.1%
United Kingdom	39.8%	38.0%	1.8%
United States	50.5%	44.6%	5.9%



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

	July	June	Change
Australia	0.74%	0.47%	0.27%
Austria	2.21%	1.15%	1.06%
Belgium	0.48%	0.32%	0.16%
Canada	1.39%	0.62%	0.77%
China	2.26%	1.90%	0.36%
France	1.89%	0.94%	0.95%
Germany	2.90%	1.87%	1.03%
Hong Kong	2.70%	1.53%	1.17%
India	5.29%	3.21%	2.08%
Ireland	1.71%	0.70%	1.01%
Israel	1.30%	1.06%	0.24%
Italy	1.87%	1.42%	0.45%
Japan	0.83%	0.25%	0.58%
Netherlands	0.51%	0.27%	0.24%
Singapore	2.17%	1.37%	0.80%
Spain	1.17%	0.84%	0.33%
Sweden	0.25%	0.29%	-0.04%
Switzerland	3.11%	1.66%	1.45%
United Arab Emirates	3.12%	2.00%	1.12%
United Kingdom	1.26%	0.71%	0.55%
United States	1.51%	0.81%	0.70%



**Annexe III : Pourcentage de spam par secteur d'activité (juillet 2007)**

	July	June	Change
Accom/Catering	38.1%	34.4%	3.7%
Agriculture	66.8%	64.1%	2.7%
Building/Cons	31.6%	30.5%	1.1%
Business Support Services	42.9%	37.3%	5.6%
Chem/Pharm	42.5%	40.0%	2.5%
Education	53.8%	52.4%	1.4%
Estate Agents	31.8%	32.9%	-1.1%
Finance	29.3%	27.6%	1.7%
General Services	34.3%	30.3%	4.0%
Gov/Public Sector	39.9%	36.9%	3.0%
Health Care	49.1%	44.5%	4.6%
IT Services	48.7%	49.9%	-1.2%
Manufacturing	57.1%	53.2%	3.9%
Marketing/Media	50.9%	47.3%	3.6%
Mineral/Fuel	38.9%	41.4%	-2.5%
Non-Profit	44.2%	33.9%	10.3%
Prof Services	41.0%	41.5%	-0.5%
Recreation	37.9%	37.9%	0.0%
Retail	42.2%	38.5%	3.7%
Telecoms	42.3%	35.5%	6.8%
Transport/Util	39.0%	42.6%	-3.6%
Wholesale	46.3%	44.9%	1.4%



**Annexe IV : Pourcentage de virus par secteur d'activité (juillet 2007)**

	July	June	Change
Accom/Catering	1.35%	0.76%	0.59%
Agriculture	0.33%	0.18%	0.15%
Building/Cons	0.82%	0.41%	0.41%
Business Support Services	0.50%	0.31%	0.19%
Chem/Pharm	2.70%	1.45%	1.25%
Education	2.53%	0.75%	1.78%
Estate Agents	0.99%	0.81%	0.18%
Finance	0.88%	1.17%	-0.29%
General Services	0.96%	0.36%	0.60%
Gov/Public Sector	0.83%	0.46%	0.37%
Health Care	1.25%	0.60%	0.65%
IT Services	1.58%	0.77%	0.81%
Manufacturing	1.47%	0.80%	0.67%
Marketing/Media	1.43%	0.67%	0.76%
Mineral/Fuel	1.33%	0.63%	0.70%
Non-Profit	1.04%	0.48%	0.56%
Prof Services	1.70%	0.79%	0.91%
Recreation	1.04%	0.68%	0.36%
Retail	1.95%	0.87%	1.08%
Telecoms	0.29%	0.15%	0.14%
Transport/Util	1.20%	0.55%	0.65%
Wholesale	1.62%	1.35%	0.27%