MessageLabs Intelligence: September 2006

"Beware of Geeks Bearing Spam"
A Review of Quarter 3/2006

Introduction

Welcome to the September edition of the MessageLabs Intelligence monthly report. This report provides the latest threat trends for September 2006, as well as a quarterly retrospective, to keep you informed regarding the ongoing fight against viruses, spam and other unwelcome content.

Top line results of this report include:

Spam – 64.4% in September (a decrease of 0.1% since August)
Viruses – One in 89.6 emails in September contained malware (an increase of 0.1% since August)
Phishing – One in 170 emails comprised a phishing attack (an increase of 0.27% since August)

Spam

In recent weeks MessageLabs has noticed an increase in the number of spam emails that are specifically targeting individuals within the technology sector by using social engineering techniques. Called "geek spam," this type of spam includes technology-related keywords within the email to dupe recipients into believing that the spam is actually something more relevant, such as a bug report. The use of technology buzzwords hidden inside the body of the spam can ensure that the email looks convincing enough for the anti-spam software to allow the mail through, and can help to pollute the Bayesian filters often used by this sector.

As threat techniques continue to increase in numbers, so do the number of prolific legal cases. In September, the popular and well known anti-spam organization Spamhaus were ordered to pay $11,715,000 in damages by the US District Court for the Northern District of Illinois to e360insight, which filed a lawsuit against Spamhaus earlier in the year suggesting that Spamhaus was breaking the law by listing e360insight in the Spamhaus Block List.

In a statement on its website, Spamhaus said, "Default judgments obtained in US county, state or federal courts have no validity in the UK and can not be enforced under the British legal system. As spamming is illegal in the UK, an Illinois court ordering a British organization to stop blocking incoming Illinois spam in Britain goes contrary to UK law which orders all spammers to cease sending spam in the first place." Although ostensibly this ruling seems to strike a blow for the spammers, it is extremely unlikely that this judgment will have any impact on Spamhaus.

In another legal case, the Security and Exchange Commission (SEC) in the US charged a number of people with using a "pump-and-dump" spam scheme to artificially inflate share prices. Jeffery Steven Stone and his wife acquired 288 million shares of stock worth around $1 million in a San Francisco-based company called WebSky Inc. The scheme operated through spam emails that hyped the stock's real value, suggesting to potential victims that the company would generate around $40 million in annual revenues. As a result of the fraud, WebSky's stock price soared by over 300% on trading volume almost 20 times greater than normal, after which Stone and his wife sold their WebSky shares. Douglas Haffer, the CEO of WebSky has also been sued by the SEC for subsequently selling shares to an entity controlled by Stone, without registering the transaction appropriately.

Viruses & Phishing
Malware attacks against Massively Multiplayer Online Role-Playing Games (MMORPG) such as World of Warcraft seem to becoming increasingly more common. The potential to turn lucrative virtual artifacts and online in-game currency into real cash has proved too attractive for the more contemporary organized criminals, who are continually looking for new ways to make money.

Such attacks may come in the form of phishing emails where gaining access to an individuals' character online may reap significant rewards. Other attacks include trojans, disguised as add-ons to enhance a character in some way, for example. These trojans may covertly steal personal data that can be used by the criminals in the pursuit of their activities. Phishing attacks now account for 52.4% of all email-based malware, and now not only target traditional banks, but also other commercial sites as well as accounts for AOL and MSN, for example.

Indeed, this has led to a new generation of sweat-shops. Rather then manufacturing textiles and clothing for the Western markets, there are now "sweat-shops" operating in certain countries that hire people for very little money to play these MMORPG games 24-hours per day. The sweat-shop farmers will sell in-game currency or virtual goods to Westerners willing to part with real cash and regularly take part in online campaigns to earn in-game currency or in some extreme cases, by mugging other players of their prized magic items, for example.

As online criminals are seemingly now taking an interest in these virtual economies as a means to laundering their criminal cash-flow using the in-game currency, MMORPGs such as Second Life have also attracted the attention of the Inland Revenue Service (IRS) in the US, as people are increasingly using a virtual life to generate a very real income from buying and selling virtual goods online.

Web traffic
Web-browsing in the workplace can cause untold problems for businesses as many more companies now report that they have experienced one or more internal security problems. One of the biggest risks now facing businesses comes from internal threats, such as uncontrolled web browsing, rather than external threats from malware and hackers. This trend has also affected the way IT decision makers position their top security concerns, which should now include internal threats.

In a report from Mitre, a US government-funded research organization, "cross-site scripting" (XSS) vulnerabilities are now apparently far more popular than buffer overflows. The increasing use of XSS bugs highlights how attackers are taking a closer interest in languages mainly intended for creating web-based applications, such as Java, .Net and PHP.

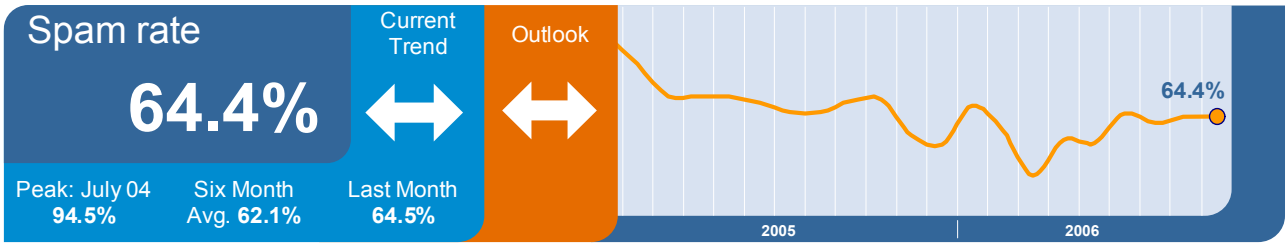
Such languages generally include "same-origin" policies, which permit interaction between different pages as long as they originate from the same domain via the same protocol. XSS bugs allow maliciously created pages, such as phishing sites to find ways around these policies, in order to gain access to personal data or data stored in other browser windows.

This edition of the MessageLabs Intelligence report is the first report to include data gathered from MessageLabs Web Security Services version 2.0, based on MessageLabs proprietary Skeptic technology, launched earlier in the year. In coming months, MessageLabs Converged Threat Analysis™ will provide the very latest intelligence and information on the most recent email and web security threats.

Global Trends & Content Analysis

MessageLabs Anti-Spam and Anti-Virus Services focus on identifying and averting unwanted communications originating from unknown bad sources and which are addressed to valid email recipients.

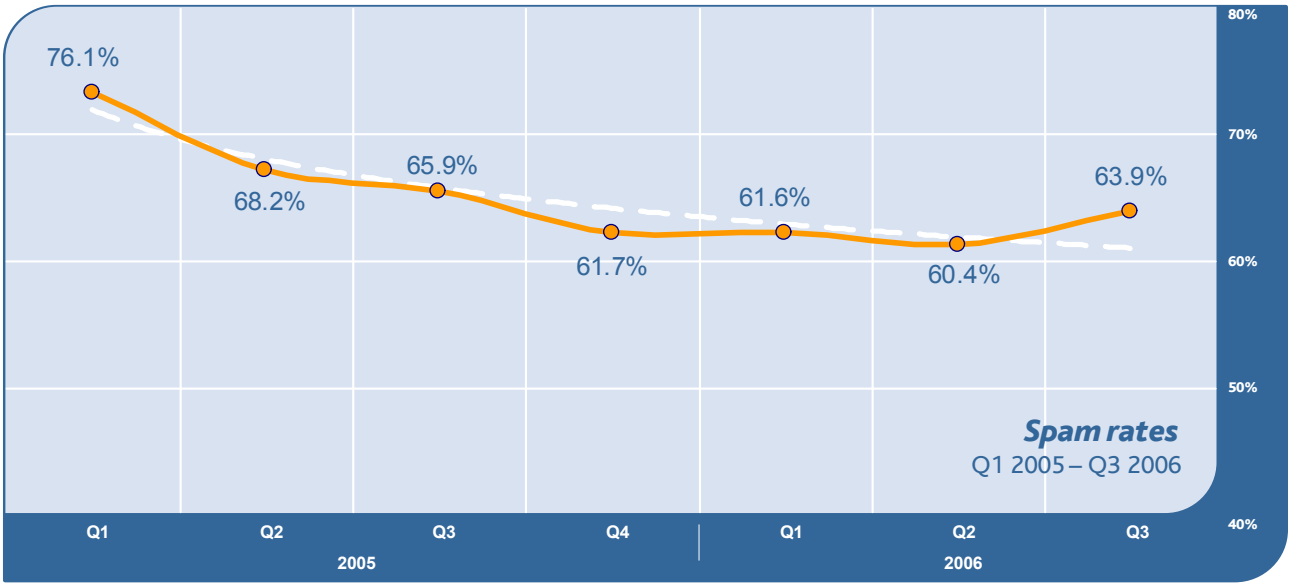
Skeptic™ Anti-Spam Protection: In September 2006, the global ratio of spam in email traffic from new and unknown bad sources, for which the recipient addresses were deemed valid, was 64.4% (1 in 1.55 emails), a decrease of 0.1% on the previous month.



The figure of 64.4% is actually a lower than the "true" spam figure. In early 2005, MessageLabs deployed an additional layer of defense at its network perimeter, known as Traffic Management. This enables us to control the amount of bandwidth that we give to absolutely known bad-sources of spam, and then to throttle those connections, slowing them down to a crawl so that to the spammer, they appear to be talking to a very slow modem.

This in turn makes it incredibly painful for spammers attempting to send their spam to MessageLabs clients as we are effectively pushing back the spam to their networks by slowing-down their ability to send lots of spam. Consequently, many such connections eventually "time-out" or move on to softer targets. **If we look at the amount of spam hitting our honey-pots, which are unprotected by comparison, this figure would be much closer to 82.1%.** For further information, please refer to the section on Traffic Management later in this report.

Quarterly Review: From the chart below, it can be seen that spam levels intercepted by MessageLabs in Q3 2006 are not as high as the same period in 2005. In that time, the techniques adopted by spammers have become increasingly more sophisticated and it can be seen that there has been a small increase between Q2 and Q3 of this year, rather than the steady decline witnessed for the same period in 2005. This is indicative that spam is not going away, and that concentrations are expected to increase again in coming months as spammers continue to adopt new techniques.

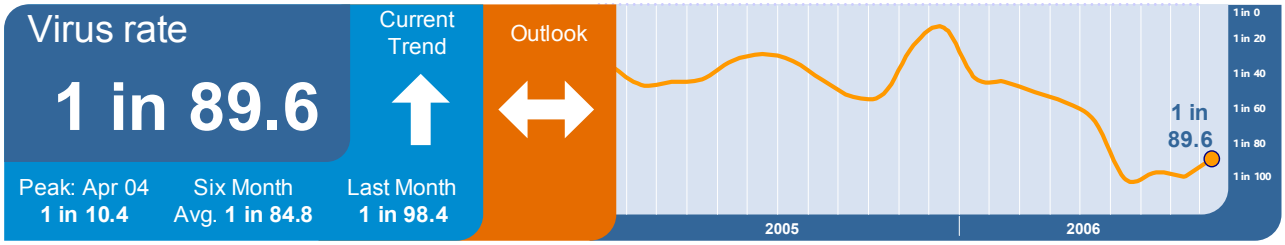


Geek Spam: In recent weeks MessageLabs has noticed an increase in the number of spam emails that use 'techno-babble' usually only associated with particular technology strands as a means of social engineering. Not only do messages with enticing subject lines, such as "Bug #33006: Your review is necessary," find their way into programmers' inboxes, but there is also a suggestion that these emails may be deliberately targeted so as to be appealing to these particular groups.

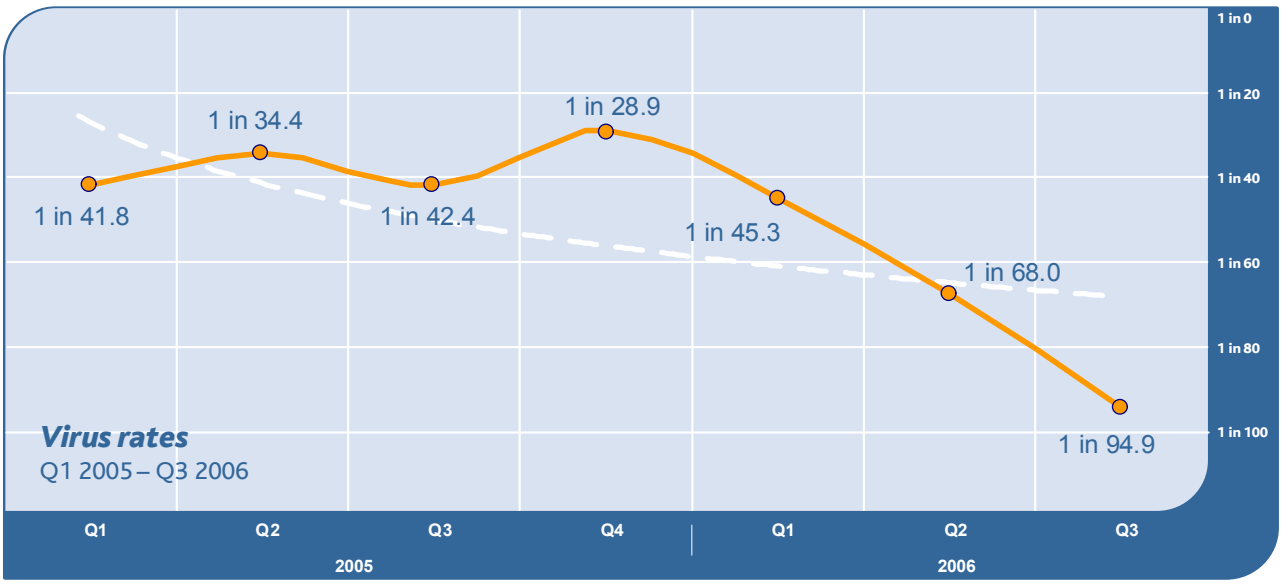
In another twist, the "geek" demographic seems to be particularly susceptible to this type of spam, in that the Bayesian filters so often employed by such techies can be easily polluted with technology buzzwords secreted into the body of the spam, such as ".NET," "cpan", "xss", "Java" etc.

What does the future hold in this area? We can almost certainly expect an increase in other similarly targeted spam, perhaps aimed at specific markets, such as Accountants, using technical financial terminology buried in the message so as to trick the recipient into not only receiving it through their anti-spam countermeasures, but also into opening it.

Skeptic™ Anti-Virus and Trojan Protection: The global ratio of email-borne viruses in email traffic from new and previously unknown bad sources destined for valid recipients, was 1 in 89.6 emails (1.12%) in September, an increase of 0.1% since last month.



Quarterly Review: During the last four quarters, virus and trojan traffic levels have steadily declined, with Q3 2006 seeing rates of 1 in 94.9 emails.



Compared with the same period in 2005, virus levels have fallen considerably over the course of this year, however, the current levels are still high enough to remain vigilant.

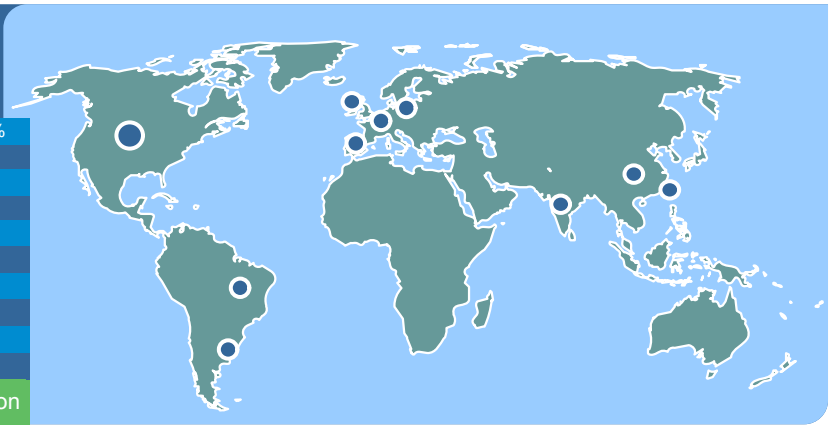
In 2006, MessageLabs has also seen a marked shift in the way online criminals are distributing their malware, in that the proportion of executable-type attachments has declined, giving way to more social engineering attacks like phishing and the inclusion of a link to a website hosting malicious software, which then becomes the vehicle by which the malware is installed onto victims' computers.

Bot Review: A "Botnet", or ro-**Bot net**-work, is a collection of compromised computers around the world, infected with trojan horses, or backdoor software, and united by a common command and control infrastructure. A botnet's controller ("bot herder") can control the group remotely, en masse. It can be seen from the following table that bots are increasing in number and distribution. Particularly in South American countries, such as Uruguay and Brazil, where the use of bots to distribute bank trojans and phishing scams has now escalated to such a degree as to make them the new "419-scam" of the region.

Botnets by geography

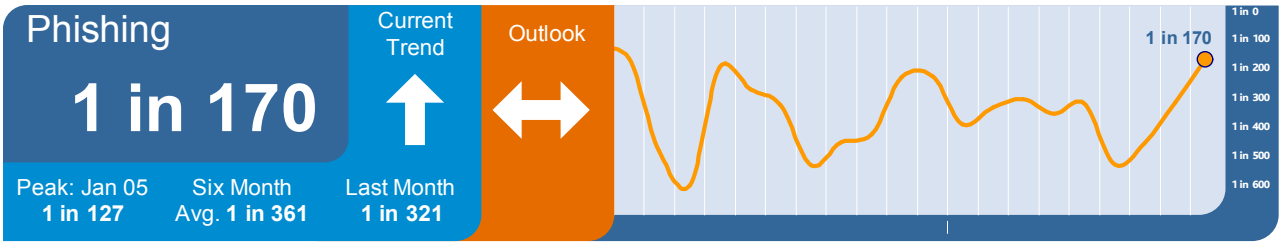
Top 10

	Q2 2006	Q3 2006
United States	10.1%	11.3%
China	9.5%	7.4%
Uruguay	3.5%	6.8%
India	8.4%	6.2%
United Kingdom	5.2%	4.8%
France	4.8%	4.8%
Germany	4.5%	4.6%
Brazil	2.8%	4.4%
Poland	2.9%	3.8%
Taiwan	3.1%	3.4%
Total bots globally		2.8 million



Phishing: September showed a large increase of 0.27% in the proportion of phishing attacks compared with the previous month. One in 170 (0.59%) emails was some form of phishing attack.

When judged as a proportion of all email-borne threats such as viruses and trojans, the number of phishing emails has risen by 21.7%. Phishing attacks accounted for more than half (52.4%) of all malicious emails intercepted by MessageLabs in September.

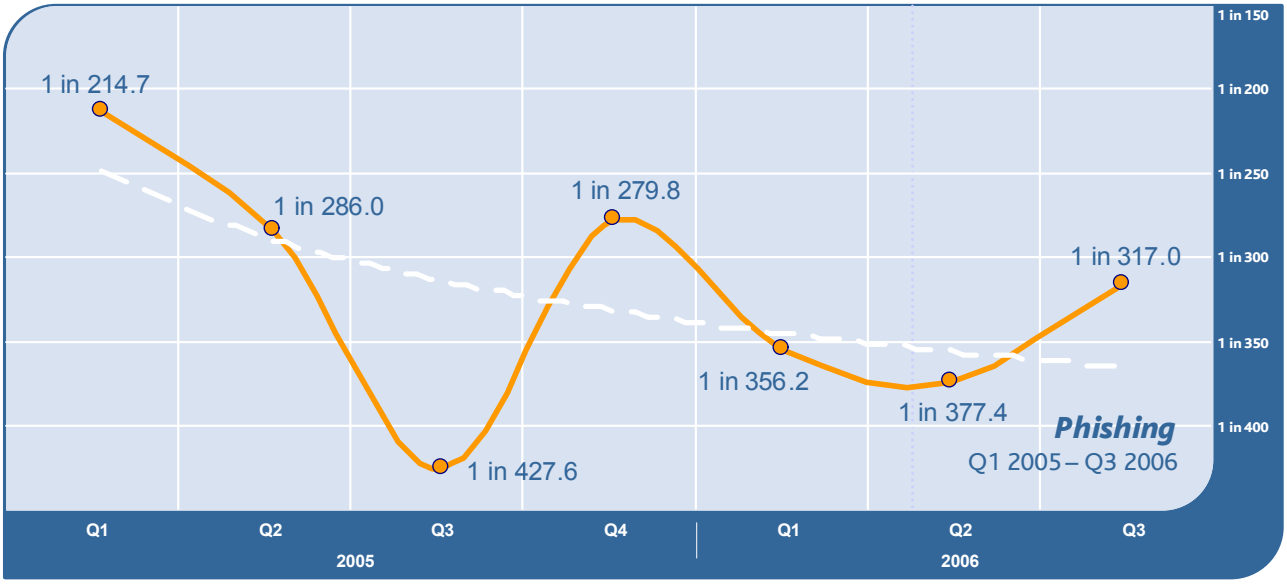


Phishing attacks continue to become more targeted as more criminal groups shift their attention from creating malware to conducting phishing attacks. The nature of these attacks has also changed in recent months, as the main organizations now being targeted have become those banks that have not currently deployed any two-factor authentication security measures. The unilateral approach undertaken by some banking organizations has indirectly resulted in a huge increase in the phishing attacks directed against those banks that may still be investigating such technology. Those banks that have deployed this technology are still being subjected to attacks, but on a much lesser scale.

These increased attacks are perhaps a prelude to the imminent release of Microsoft Internet Explorer 7.0, which will

include additional anti-phishing countermeasures. Already, MessageLabs has seen examples of specially crafted bank trojans that are being sold on the Internet, which can be customized for as little as USD $800 to target any online banking website. The trojan approach works by monitoring browser addresses and when the victim visits a target site, the trojan will wait for the user to complete the authentication process before hijacking the session and handing control to the criminals.

Quarterly Review: The average ratio of phishing emails for the quarter has increased between Q2 and Q3, halting the previous downturn.



Skeptic™ Web Security Version 2.0: In July 2006, MessageLabs launched version 2.0 of its Web Security Services. Skeptic Web Security paves the way for the introduction of MessageLabs Converged Threat Analysis™, taking the very latest threat and reputation information from other protocols, such as email, and applying that knowledge to web traffic.

In the chart below it can be seen that the most common trigger for policy-based filtering, applied by MessageLabs for its business clients, is Advertisements & Popups (90.1%). The "Unclassified" category identifies new and previously uncategorized sites that may potentially need to be prohibited. The "Unclassified" category affords more confidence when defining new rules, which means that newly detected malicious sites may be handled more appropriately until categorized, thereby safeguarding against sites which appear and disappear within a 24 to 48 hour timeframe; such sites may be used for disreputable purposes, such as hosting phishing and spam sites, information stealing trojans and other fraudulent activities.

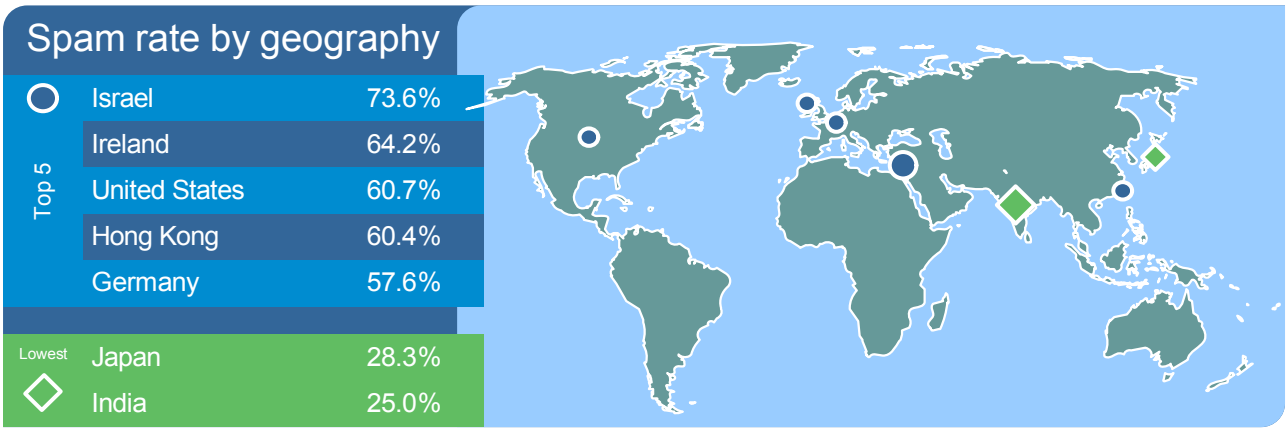
Web Security Services (Version 2.0) Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisements & Popups	90.1%	Trojan-Clicker.HTMLAgent.a	35.4%	Adware-180SA	40.9%
Streaming Media	3.3%	Generic Downloader.o	13.5%	Adware-ISTBar	34.8%
Downloads	1.2%	JS/Wonka	10.2%	Adware-Lop	6.1%
Unclassified	1.2%	Trojan-Downloader.HTMLAgent.aq	5.6%	Adware-GAIN	6.1%
Adult/Sexually Explicit	0.8%	W32/VBS_Malware	5.2%	Adware-Look2Me	3.0%
Web-based E-mail	0.5%	Suspicious IFrame -c	1.6%	Adware-abetterintrnt.dldr	3.0%
Chat	0.5%	Trojan-Downloader.Win32.Agent.alr	1.5%	Adware-UCMore	1.5%
Shopping	0.4%	Trojan-Downloader.JS.Agent.ac	1.5%	Adware-PurityScan	1.5%
Blogs & Forums	0.4%	Trojan-Downloader.Win32.Small.cpg	1.3%	Adware-abetterintrnt.gen.a	1.5%
Personals & Dating	0.3%	Trojan-Downloader.JS.Agent.ap	1.2%	Adware-ISTbar.b	1.5%
Other	1.4%	Other	23.0%		

Analysis of web security activity also shows that 99.7% of interceptions occur as the result of a rule triggered by a policy which has been implemented by a system administrator. However, 0.3% of interceptions are also the result of malware or potentially unwanted programs, including adware and spyware that was detected heuristically by Skeptic Web Security Services version 2.0.

Geographical Breakdown: Based on Targeted Countries

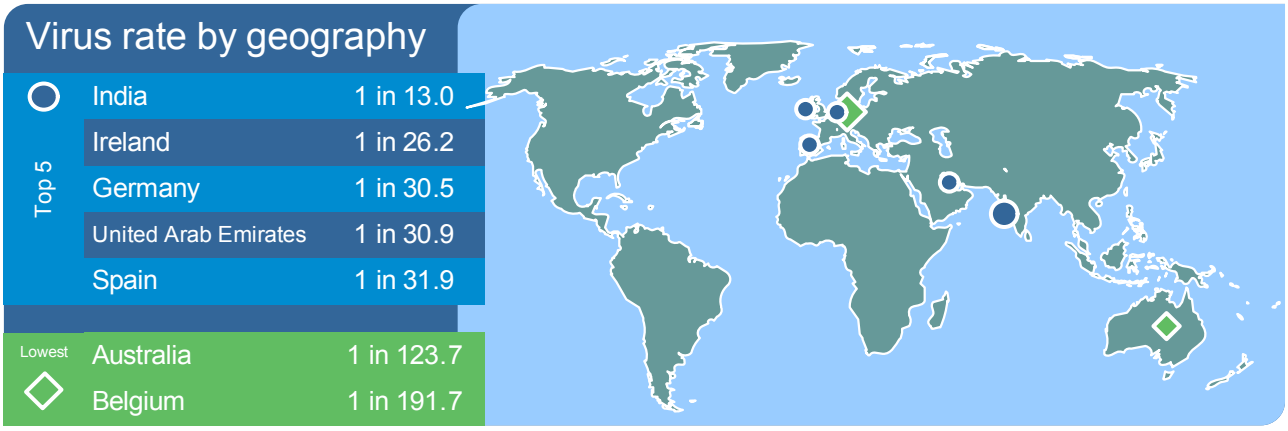
Monthly Analysis: By analyzing the geographical dispersal of email traffic where possible, MessageLabs compiles data that shows the impact and vulnerability rates of spam and viruses specific to geographies. The charts below reflect impact and ratios for September 2006.



Although Israel continues to bear the burden of being targeted with the highest ratio of spam in September, spam levels actually dropped by 4.4% when compared with August.

The greatest decline in the top-5 countries came in Hong Kong, where spam levels fell by 5.9% compared with August. Overall, the largest drop was in Italy (ranked 7th), which fell by 24% to 54% in September.

Of the top-5 countries, Ireland suffered the largest increase by 1.7% from August, however the largest increase overall was in Singapore (ranked 6th), where levels rose by 9.2% to 55.4% in September.



Again India continues to be targeted with the highest ratio of virus traffic versus other countries, with levels actually

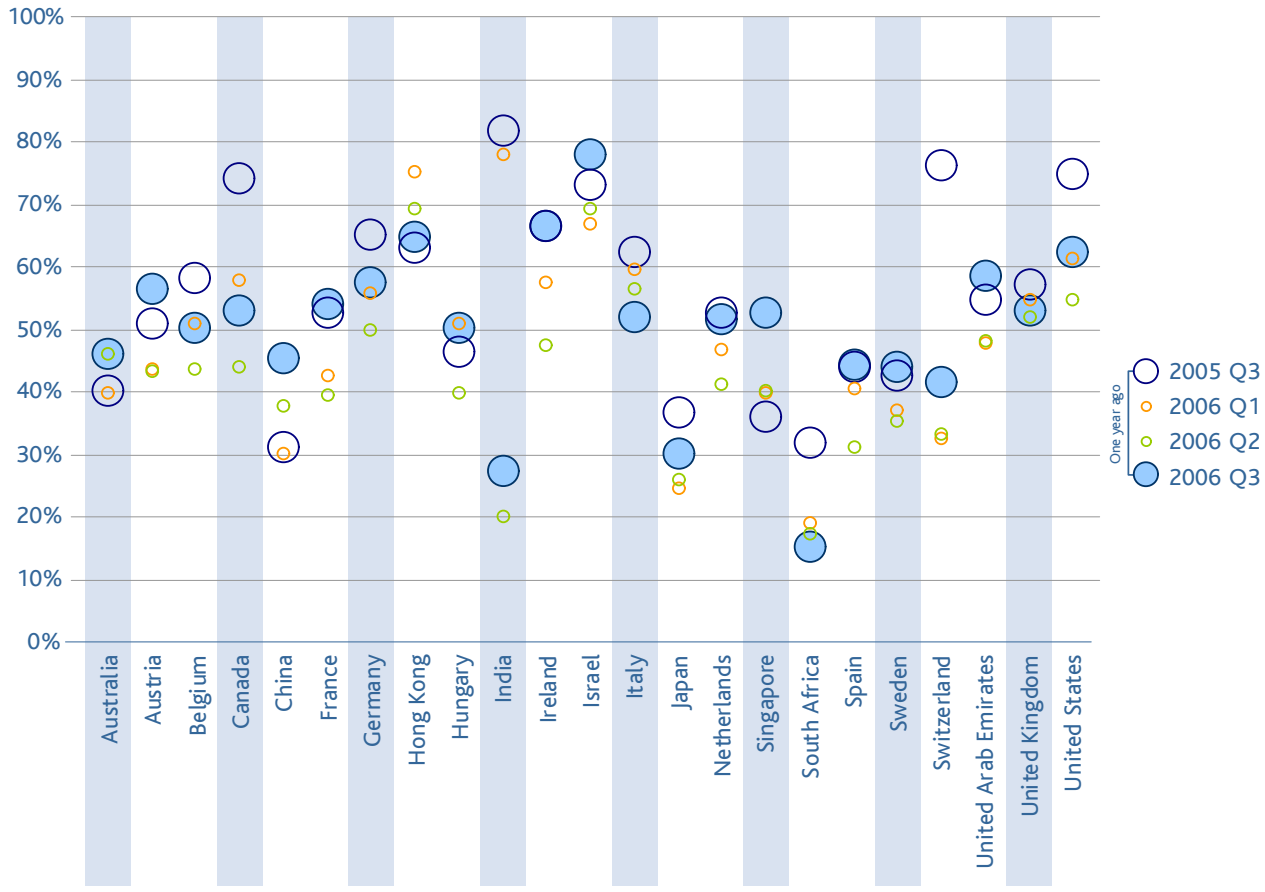
increasing by a further 0.2% compared with August.

The greatest decline in the top-5 countries and overall, was observed in Germany, where virus traffic fell by 1.4% compared with August.

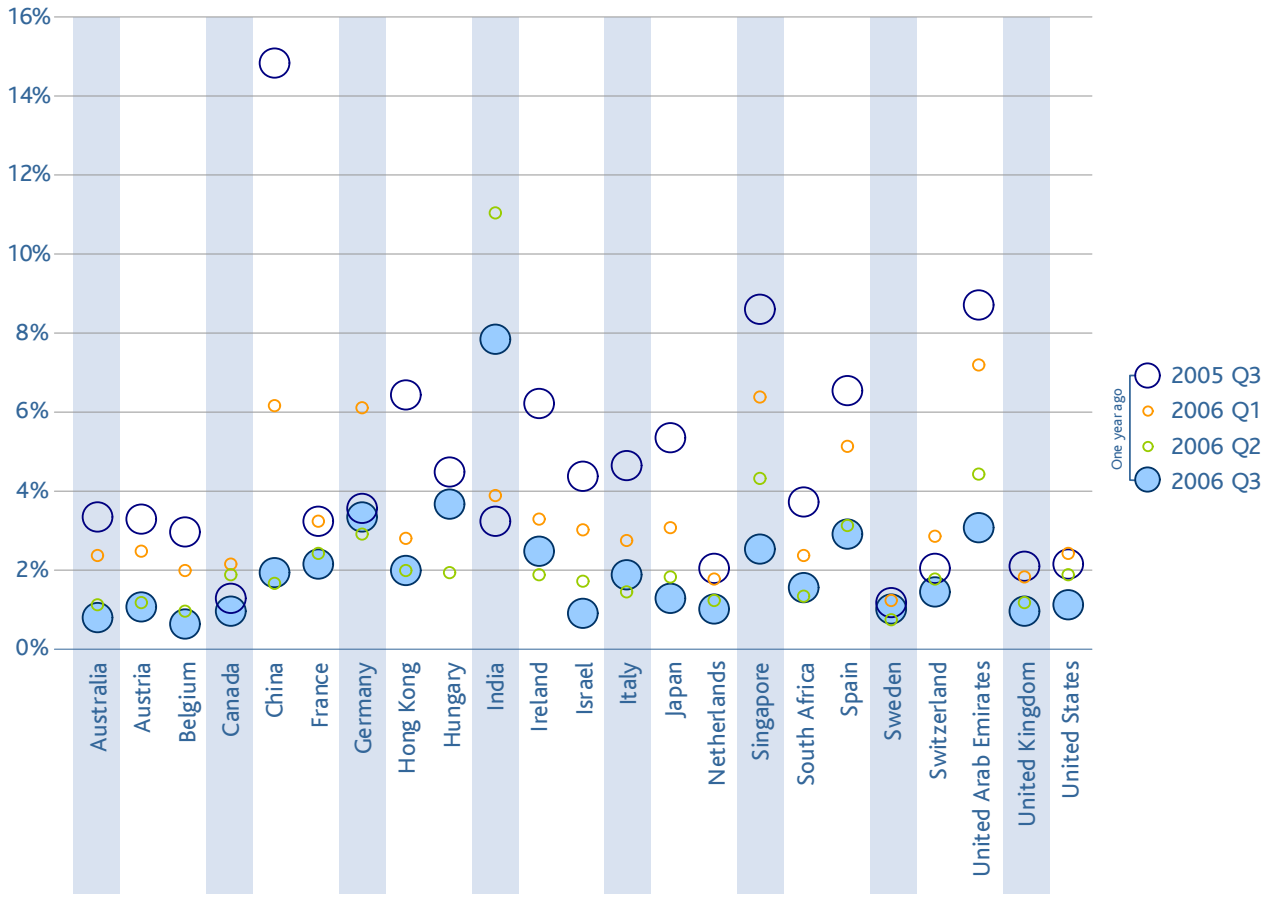
Of the top-5 countries and overall, Ireland suffered the largest increase by 1.2% when compared with the August figures.

Quarterly Review: The charts below have been specifically designed in order to highlight the interesting insights gained by comparing quarter on quarter changes, but also the Q3 figures with the same period in 2005. Data for these charts last month can be found in the Appendix at the end of this report.

Spam Rate by Geography (2006 Q1, Q2, Q3 and 2005 Q3)



Virus Rate by Geography (2006 Q1, Q2, Q3 and 2005 Q3)



Vertical Industry Breakdown

Monthly Analysis: By analyzing the market distribution of email traffic where possible, MessageLabs compiles data that shows the impact and vulnerability rates of spam and viruses specific to major industry sectors. The charts below reflect impacts and ratios for September 2006.

Spam rate by vertical

Top 5	Education	62.9%
	Manufacturing	62.3%
	Telecoms	60.1%
	Recreation	58.9%
	Transport /Util	57.7%
Lowest	Finance	46.7%
	Gov/Public Sector	40.7%

Virus rate by vertical

Top 5	Business Support Services	1 in 14.3
	Wholesale	1 in 33.9
	Education	1 in 41.8
	Manufacturing	1 in 64.3
	Non-Profit	1 in 65.1
Lowest	IT Services	1 in 140.1
	Telecoms	1 in 183.7

For spam, the Education sector remains the main target, with a higher ratio of spam than other sectors. Spam levels have actually risen by 11% when compared with last months figures, representing the greatest increase within the top-5 sectors.

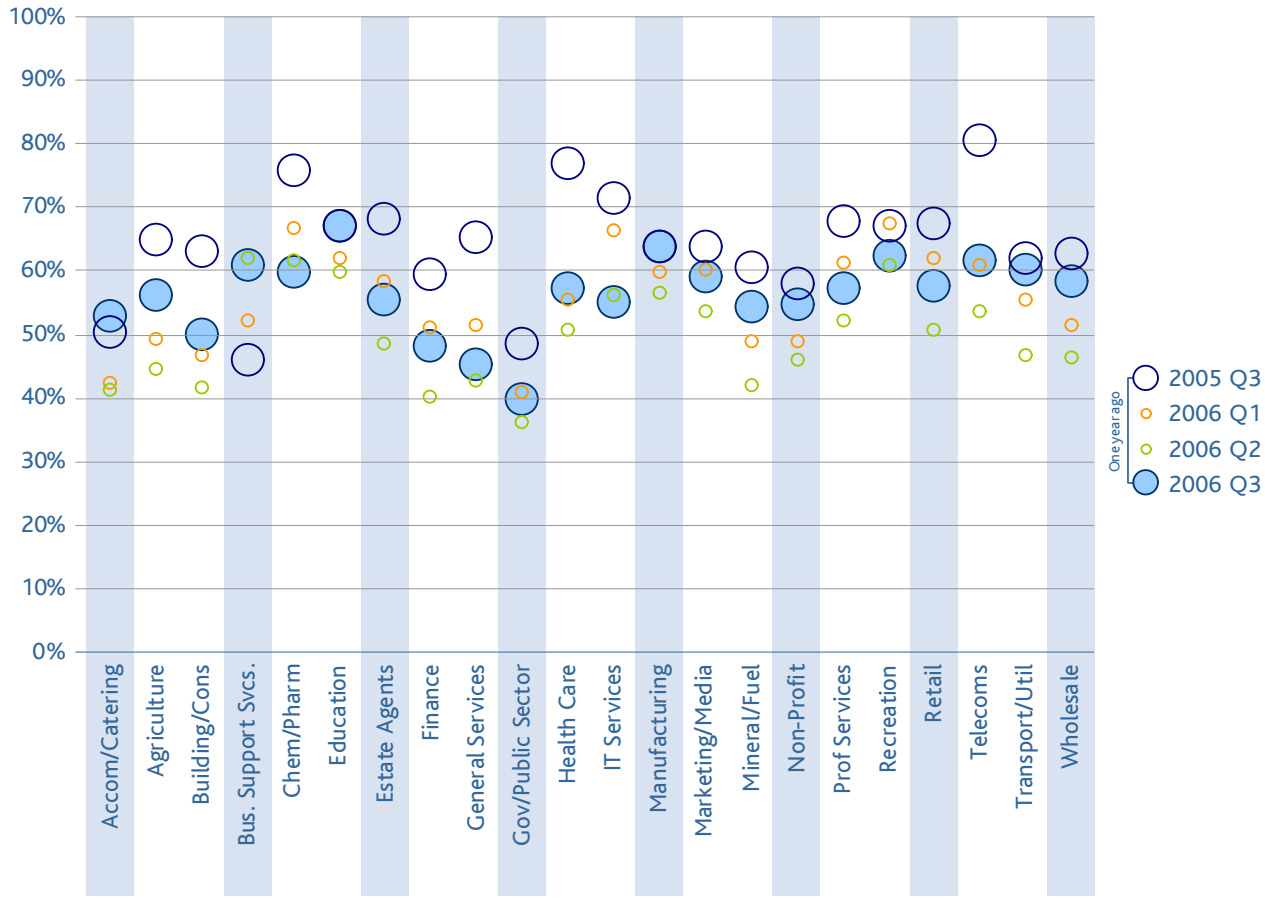
Overall, the largest rise was seen in the General Services sector (ranked 15th), which rose by 13.5% to 53.5% in September. The greatest decline in the top-5 sectors came in Recreation, where spam levels fell by 5.9% compared with the previous month. Overall, the largest drop came in the Chemical & Pharmaceutical sector (ranked 6th), which fell by 10.6% to 57.6% in September.

For viruses, Business Support Services remains the dominant focus of activity, with a higher ratio of viruses than other sectors, with virus traffic rising by 0.1% since August. The greatest increase within the top-5 sectors and overall was seen in the Education sector, where levels rose by 0.5% in September.

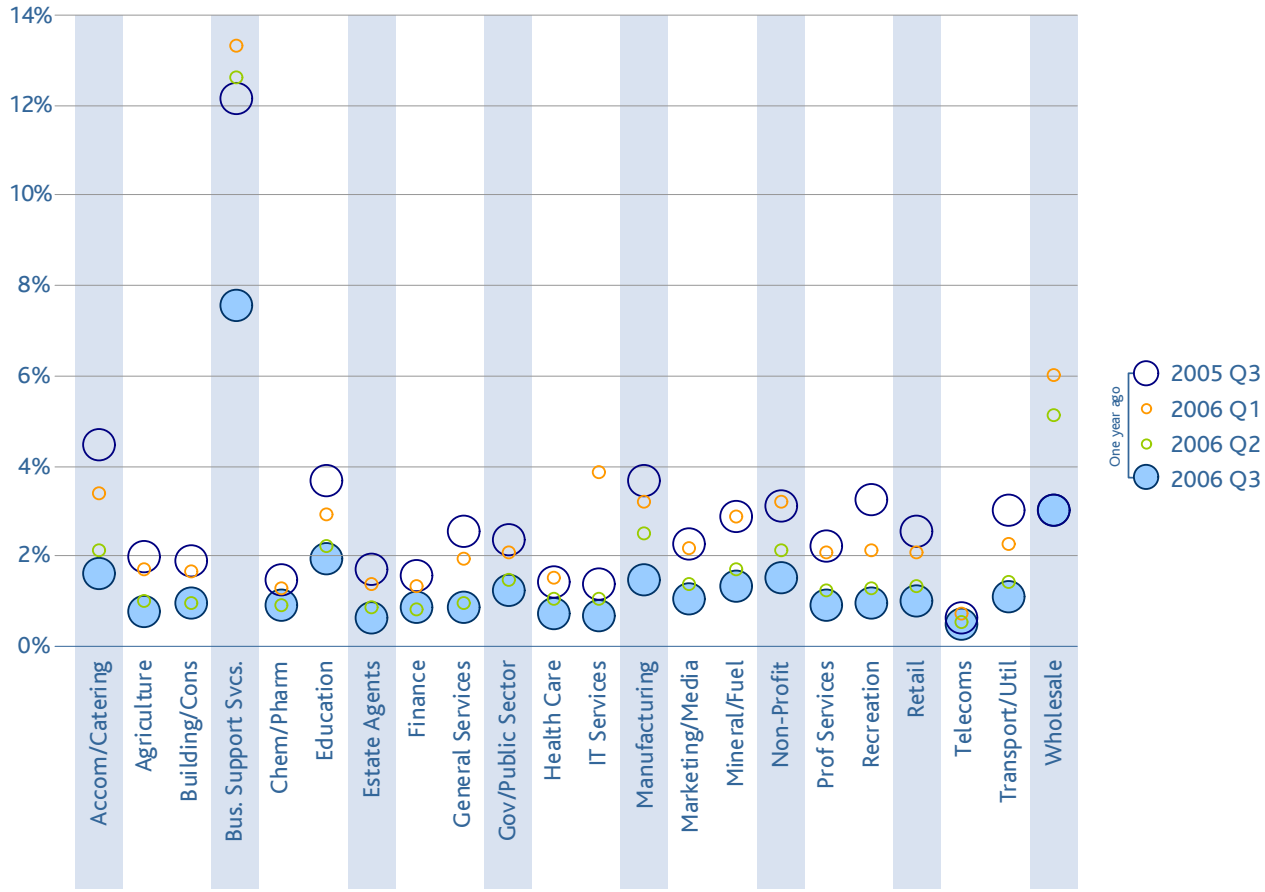
The largest drop across the top-5 sectors was in the Wholesale sector, where virus levels fell by 0.2% compared with the previous month. Overall, the largest drop came in the Building & Construction sector (ranked 16th), where levels fell by 5.9% to 1 in 101.5 (1%) in September.

Quarterly Review: The following charts highlight the interesting insights that last month be gained by comparing quarter on quarter changes, as well comparing the Q3 figures with the same period in 2005.

Spam Rate by Vertical (2006 Q1, Q2, Q3 and 2005 Q3)



Virus Rate by Vertical (2006 Q1, Q2, Q3 and 2005 Q3)



Traffic Management (Protocol Level)

Traffic Management continues to reduce the overall message volume through techniques operating at the protocol level. Unwanted senders are identified and connections to the mail server are slowed down using features embedded in the TCP protocol. Incoming volumes of known spam are significantly slowed, while ensuring legitimate email is expedited.

Connection Management

Connection Management is particularly effective in stopping directory harvest, brute force and email denial of service attacks, where unwanted senders send high volumes of messages to force spam into an organization or disrupt business communications.

Connection Management works at the SMTP level using techniques that verify legitimate connections to the mail server, and is comprised of the following:

SMTP Validation: Identifies unwanted email originating from known spam and virus sending sources, where the source can unequivocally be identified as an open proxy or a botnet, and rejects the connection accordingly. In September, an average of 5.1% of inbound messages were intercepted from botnets and other known malicious sources and rejected as a consequence.

Registered User Address Validation: Reduces the overall volume of emails for registered domains, by discarding connections for which the recipients are identified as invalid or non-existent. In September, an average of 11.9% of recipient addresses were identified as invalid; these were attempted directory attacks upon domains that were therefore prevented.

The table below details the current impact of connection management techniques on unwanted email volume being measured by MessageLabs Intelligence. Without these additional multiple layers of defense, spam traffic destined for MessageLabs clients in September would otherwise account for around 82.1% of global email traffic, a decrease of 2.8% on the previous month.

Region	SMTP Validation *(botnet sources)*	User Validation *(directory attacks)*
USA	4.70%	12.20%
UK	5.60%	12.10%
Europe	5.60%	11.40%
Asia Pacific	3.80%	7.90%
Worldwide	**5.10%**	**11.90%**

Effects of Connection Management Techniques

MessageLabs is a leading provider of integrated messaging and web security services, with over 15,000 clients ranging from small business to the Fortune 500 located in more than 80 countries. MessageLabs provides a range of managed security services to protect, control, encrypt and archive communications across Email, Web and Instant Messaging.

These services are delivered by MessageLabs globally distributed infrastructure and supported 24/7 by security experts. This provides a convenient and cost-effective solution for managing and reducing risk and providing certainty in the exchange of business information. For more information, please visit www.messagelabs.com.

For further information on MessageLabs Intelligence, please visit www.messagelabs.com/intelligence and register to receive regular alerts and reports.

NB: All figures mentioned in this report were correct at the time of going to press.

Appendices

Appendix I: Spam Rate by Geography (2006 Q1, Q2, Q3 and 2005 Q3)

	Q3 05	Q1 06	Q2 06	Q3 06
Australia	39.99%	39.70%	45.70%	45.79%
Austria	50.86%	43.60%	43.00%	56.12%
Belgium	57.83%	50.60%	43.40%	50.12%
Canada	73.79%	57.70%	43.70%	52.94%
China	31.02%	30.00%	37.50%	45.04%
France	52.42%	42.40%	39.40%	53.81%
Germany	64.94%	55.50%	49.80%	57.42%
Hong Kong	62.72%	75.10%	69.20%	64.63%
Hungary	46.04%	50.90%	39.40%	50.08%
India	81.69%	77.70%	19.70%	27.22%
Ireland	66.37%	57.30%	47.10%	66.43%
Israel	72.96%	66.70%	69.10%	77.61%
Italy	62.16%	59.50%	56.10%	51.60%
Japan	36.56%	24.30%	25.80%	29.83%
Netherlands	52.45%	46.50%	41.00%	51.27%
Singapore	35.82%	39.50%	40.00%	52.42%
South Africa	31.72%	18.80%	17.10%	14.94%
Spain	43.82%	40.30%	31.00%	44.09%
Sweden	42.47%	36.90%	35.00%	43.74%
Switzerland	76.04%	32.50%	32.90%	41.22%
United Arab Emirates	54.68%	47.60%	47.90%	58.19%
United Kingdom	56.99%	54.50%	51.60%	52.66%
United States	74.59%	61.00%	54.70%	62.27%

Appendix II: Virus Rate by Geography (2006 Q1, Q2, Q3 and 2005 Q3)

	Q3 05	Q1 06	Q2 06	Q3 06
Australia	3.30%	2.35%	1.09%	0.77%
Austria	3.26%	2.43%	1.16%	1.05%
Belgium	2.90%	1.94%	0.94%	0.59%
Canada	1.26%	2.13%	1.83%	0.92%
China	14.80%	6.12%	1.65%	1.89%
France	3.18%	3.18%	2.37%	2.11%
Germany	3.50%	6.06%	2.86%	3.29%
Hong Kong	6.42%	2.75%	1.95%	1.94%
Hungary	4.45%	34.46%	1.88%	3.63%
India	3.21%	3.83%	11.00%	7.79%
Ireland	6.17%	3.24%	1.83%	2.43%
Israel	4.35%	3.01%	1.66%	0.89%
Italy	4.62%	2.71%	1.41%	1.82%
Japan	5.34%	3.01%	1.82%	1.26%
Netherlands	1.99%	1.76%	1.20%	0.95%
Singapore	8.55%	6.33%	4.30%	2.49%
South Africa	3.69%	2.31%	1.31%	1.50%
Spain	6.53%	5.10%	3.12%	2.90%
Sweden	1.12%	1.17%	0.71%	1.00%
Switzerland	2.01%	2.82%	1.75%	1.42%
United Arab Emirates	8.70%	7.14%	4.39%	3.05%
United Kingdom	2.08%	1.81%	1.16%	0.95%
United States	2.11%	2.40%	1.84%	1.08%

Appendix III: Spam Rate by Vertical (2006 Q1, Q2, Q3 and 2005 Q3)

	Q3 05	Q1 06	Q2 06	Q3 06
Accom/Catering	50.16%	42.13%	41.26%	52.74%
Agriculture	64.61%	49.21%	44.41%	55.94%
Building/Cons	62.88%	46.48%	41.31%	49.75%
Bus. Support Svcs.	45.66%	52.02%	61.66%	60.62%
Chem/Pharm	75.81%	66.45%	61.59%	59.71%
Education	67.05%	61.79%	59.48%	66.99%
Estate Agents	68.07%	58.08%	48.45%	55.40%
Finance	59.12%	50.75%	40.10%	47.83%
General Services	65.14%	51.13%	42.72%	44.94%
Gov/Public Sector	48.52%	40.72%	35.95%	39.77%
Health Care	76.72%	55.20%	50.51%	56.96%
IT Services	71.23%	66.13%	56.03%	55.07%
Manufacturing	63.55%	59.76%	56.42%	63.70%
Marketing/Media	63.66%	59.92%	53.30%	58.74%
Mineral/Fuel	60.39%	48.73%	41.69%	54.21%
Non-Profit	57.75%	48.55%	45.89%	54.48%
Prof Services	67.47%	61.18%	51.98%	57.10%
Recreation	66.86%	67.23%	60.70%	62.20%
Retail	67.28%	61.76%	50.45%	57.43%
Telecoms	80.47%	60.60%	53.41%	61.44%
Transport/Util	61.85%	55.24%	46.71%	59.99%
Wholesale	62.51%	51.22%	46.12%	58.13%

Appendix IV: Virus Rate by Vertical (2006 Q1, Q2, Q3 and 2005 Q3)

	Q3 05	Q1 06	Q2 06	Q3 06
Accom/Catering	4.43%	3.38%	2.10%	1.61%
Agriculture	1.94%	1.67%	0.99%	0.76%
Building/Cons	1.88%	1.63%	0.95%	0.93%
Bus. Support Svcs.	12.13%	13.32%	12.61%	7.56%
Chem/Pharm	1.46%	1.24%	0.89%	0.91%
Education	3.64%	2.90%	2.20%	1.92%
Estate Agents	1.67%	1.35%	0.82%	0.59%
Finance	1.54%	1.32%	0.81%	0.82%
General Services	2.51%	1.91%	0.92%	0.87%
Gov/Public Sector	2.33%	2.05%	1.43%	1.20%
Health Care	1.41%	1.52%	1.04%	0.71%
IT Services	1.37%	3.84%	1.05%	0.63%
Manufacturing	3.64%	3.19%	2.50%	1.45%
Marketing/Media	2.26%	2.16%	1.35%	1.04%
Mineral/Fuel	2.86%	2.85%	1.69%	1.31%
Non-Profit	3.10%	3.18%	2.12%	1.48%
Prof Services	2.20%	2.08%	1.23%	0.87%
Recreation	3.25%	2.11%	1.28%	0.91%
Retail	2.53%	2.04%	1.30%	0.97%
Telecoms	0.60%	0.71%	0.53%	0.45%
Transport/Util	2.98%	2.25%	1.42%	1.05%
Wholesale	3.02%	6.01%	5.11%	3.00%