



MessageLabs Intelligence: June 2006

“Going Up, Going Down!” - A Review of Quarter 2/2006

Introduction

Welcome to the June edition of the MessageLabs Intelligence monthly report. This report provides the latest threat trends for June 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 – 64.8% in June (an increase of 6.9% since May)

Viruses – One in 101 emails in June contained malware (a decrease of 0.5% since May)

Phishing – One in 531 emails comprised a phishing attack (a decrease of 0.12% since May)

After a stagnant spam rate of 60% since Q4 2005, spam levels are again on the increase, however this upturn in activity is in contrast to the virus and phishing activities where levels have returned to the considerably lower levels from January 2004, around the time when MyDoom first appeared. Has the world domination approach of MyDoom and others that followed in its wake now finally changed in favor of the more targeted approach? Can we finally draw a line in the sand for mass-mailing viruses or is it more likely that bad guys are now using so many different approaches for such different target audiences?

What we can conclude is that in 2006, cyber threats have become smarter and much more targeted to evade detection for far longer.

The number of targeted trojan attacks specifically designed to purloin intellectual property from businesses and organizations has risen from one or two per week in Q2 2005, to approximately one per day in June this year (a six fold increase). These attacks are highly targeted and only appear in very low numbers, often exploiting vulnerabilities in specific applications, 69% of which were targeted at Microsoft Word.

It is certainly true that the cyber-criminals' hunger for financial gain and stolen intellectual property has fuelled the development of criminal malware at a breakneck pace. Viruses have for some time been linked with spam and phishing attacks; however, this high-octane evolution has now engulfed the application of increasingly targeted spyware. Much of the apparatus to achieve this already exists at the cutting edge where spyware has become intrinsic to the means by which bot technology now operates.

As the threats from viruses, spyware and spam further converge to become interdependent, the boundaries between them are almost impossible to distinguish: creating a pernicious triumvirate casting a longer, darker shadow for some time to come.

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.

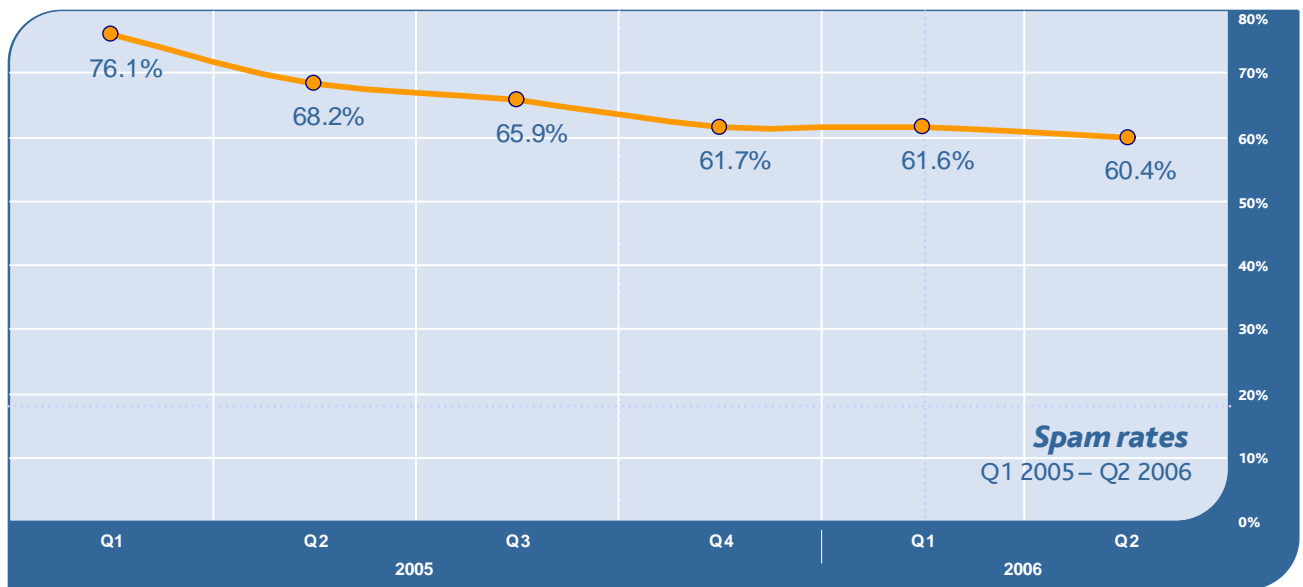
Skeptic™ Anti-Spam Protection: In June 2006, the global ratio of spam in email traffic from new and unknown bad sources, for which the recipient addresses were deemed valid, was 64.8% (1 in 1.54 emails), an increase of 6.9% on the previous month.



The figure of 64.8% is actually a little lower than the “true” spam figure. Just a little over a year ago, 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’re 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 87%. 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 Q2 2006 are not as high as the same period in 2005. This suggests that spam concentrations have reached a plateau; overall, real spam levels have not actually changed much since the same period 12 months ago, although the techniques that spammers have adopted in that time have become increasingly more sophisticated and only combated using anti-spam techniques that are effective at the Internet-level.

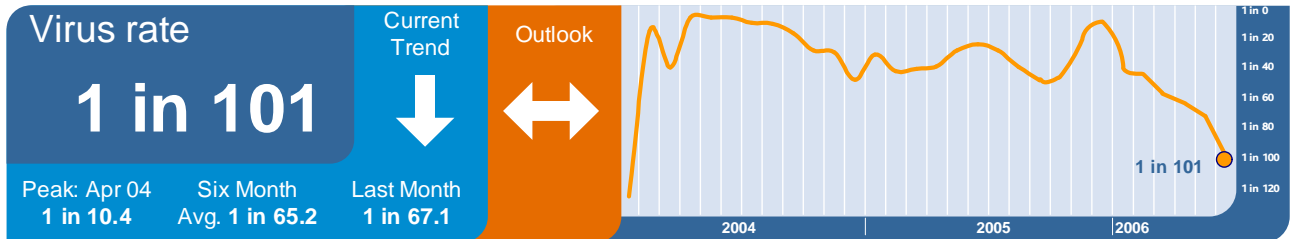


Perhaps it can be said that in recent months, “old-style” email spam has lost some of its momentum as the most effective medium for unsolicited marketing. Spammers are already turning to mobile SMS (Simple Message Service) spam, testament in at least one case earlier this year involving text messages. In February, Verizon Wireless was granted an injunction barring a travel agency based in Florida from sending unsolicited text messages to the mobile provider’s customers.

Spammers are more frequently turning to newer communications technology, polluting weblogs with comments that contain links to disposable spam domains and even creating their own “splogs” or spam-blogs. Instant Messaging (or IM) is being targeted too, with some estimating that almost 10% of IM traffic is now spam. The clock would have to be wound-back several years before such low levels were remembered for email traffic. The latest development in this evolutionary tale is in social networking environments such as the ubiquitous MySpace.com, where spammers are creating convincing profiles that contain links to seductive, but automated IM “chat-bot” sirens that typically lure unsuspecting MySpacers onto the rocks of some lucrative webcam site. These profiles are then used to send out baiting “friend requests” via specialized software that is able to target the recipients from the online profiles, and in large numbers. For example, targeting males, aged 18-24 years, located in the US. Some of these profiles have also been reported to contain bogus video links that are alleged to attempt to install spyware onto the visitors’ computers exploiting malformed media files.

All of this becomes an increasingly worrying threat for IT managers who are attempting to implement greater controls over the webs and to protect and manage Internet access within their business. Access to such sites can present its own problems, for example, blocking IM traffic at the corporate firewall may not always bring the desired results, as it is often possible to access IM clients via the web. Some sites, such as MySpace.com also have a self-contained IM interface built into the website, making it almost impossible to secure the flow of communications traffic into and out of an organization without sometimes resorting to more draconian measures.

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 101 emails (1%) in June, a decrease of 0.5% since May.



Quarterly Review: In Q2 2006, virus and trojan traffic declined from the Q1 2006 figure of 1 in 45.3 (2.2%) to 1 in 68.0 (1.5%), representing a drop of 0.7%. Compared with the Q2 2005 figure of 1 in 34.4 (2.9%), this also represents an annual drop of 1.4%.



Targeted Trojans: Twelve months ago, MessageLabs first reported intercepting low numbers of carefully crafted trojan attacks of a very dangerous kind. At the time, these attacks had been tracked at around one or two per week increasing to around three to four per week earlier in this year. In the second quarter of 2006 however, these attacks have risen and this month are now at a rate of one a day. These attacks are highly targeted, often exploiting vulnerabilities in specific applications. These types of attack are always crafted in such a way as to evade detection by traditional anti-virus software.

During the last six months, an analysis of the breakdown of application types being exploited for these purposes is: 69% .doc, 21% .chm, and only 10% .exe. In the last few weeks PowerPoint has started to rise in usage. As yet, MessageLabs has seen no sign that the recently reported Microsoft Excel vulnerabilities are being actively used. However, this is expected to change soon.

Bot Review: As botnets become more agile and harder to uncover and disrupt, the relationship between botnets and spyware is often overlooked. Botnets are generally thought of as being used to send out spam, viruses and

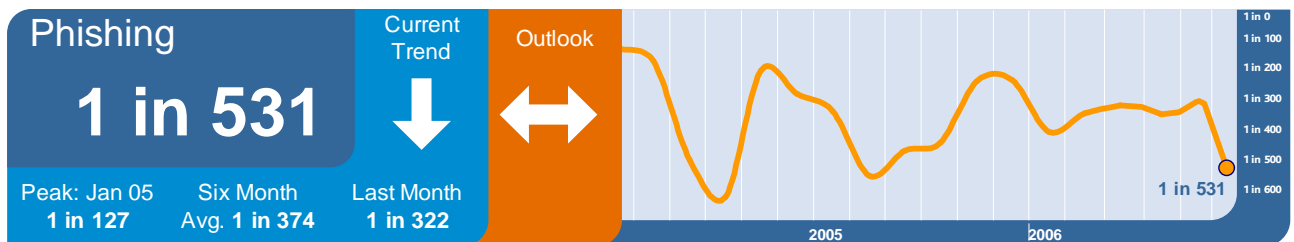
phishing attacks directly to other victims; whereas spyware conversely resides on an individual computer and harvests information about the user.

However, more recently it has been feared that with spyware deployed on the individual zombie computers within a botnet, the botnet can be used in turn to target these attacks more intelligently – targeting individuals within the botnet itself, harvesting contacts from users address books via spear-phishing emails, spam and viruses that appear to be more realistic.

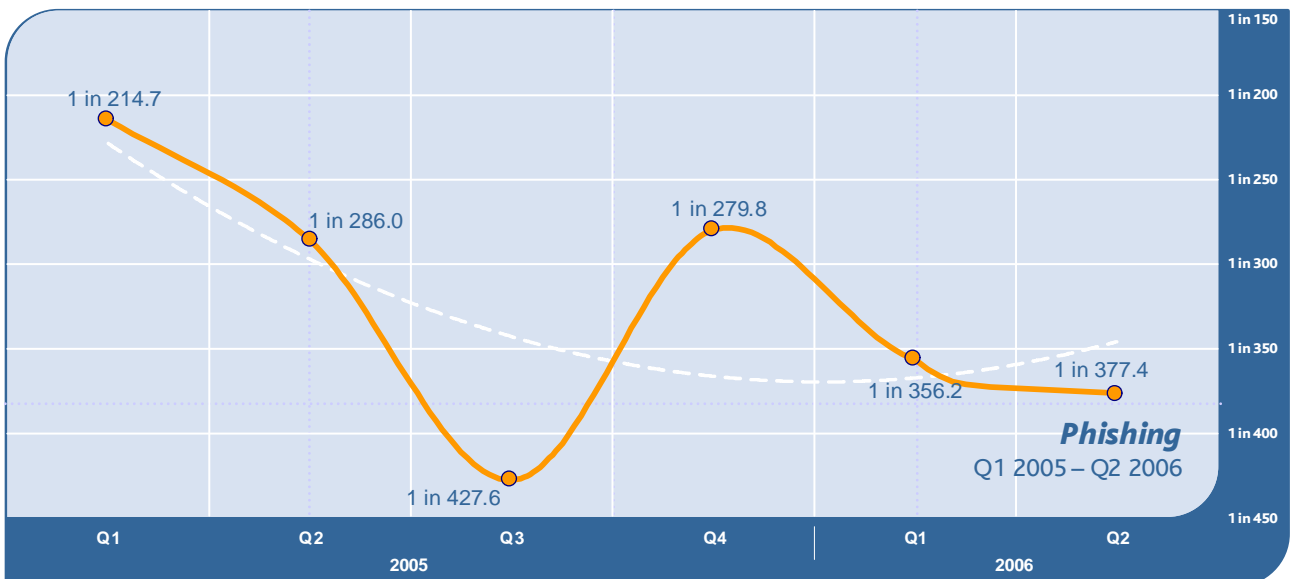
By profiling the users behind the zombie computers, the cyber-criminals can gather very personal information, such as age, sex, location, bank and websites used and use this data to target them. Whilst the traditional view of the botnet remains that spam is being sent out, but now these botnets are also being profiled as recipients.

Phishing: June showed a decrease of 0.12% in the proportion of phishing attacks compared with the previous month. One in 531 (0.19%) 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 fallen slightly by 1.8%, now accounting for 19% of all malicious emails intercepted by MessageLabs in June.



Quarterly Review: The average ratio of phishing emails for the quarter has fallen by 0.02% from 1 in 356 (0.28%) in Q1 to 1 in 377 (0.26%) in Q2.



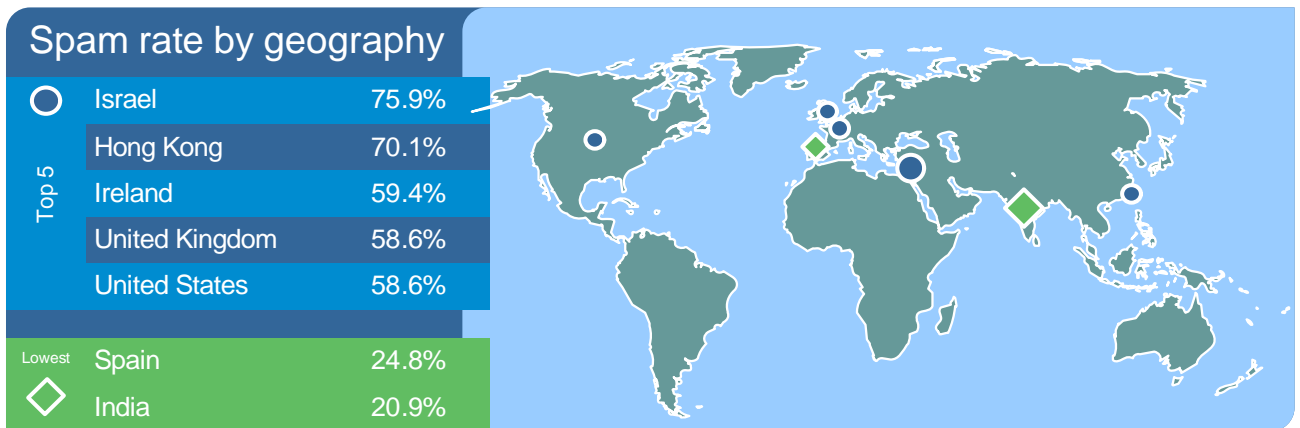
Looking at this quarter-on-quarter trend over the first half of 2006, we can see that in spite of a recent marginal decline, phishing attacks continue to become more focused as more criminal groups focus their attention from creating malware to phishing.

This is also evidenced in the analysis of phishing attacks when measured as a proportion of all malicious email traffic, including viruses and trojans; the share of which has increased by 6.5% from 12.1% in Q1 to 18.6% in Q2.

Consequently, MessageLabs continues to observe a decline in the scatter-gun approach where phishing emails used to be sent in large numbers, in favor of more subtle, selectively targeted attacks.

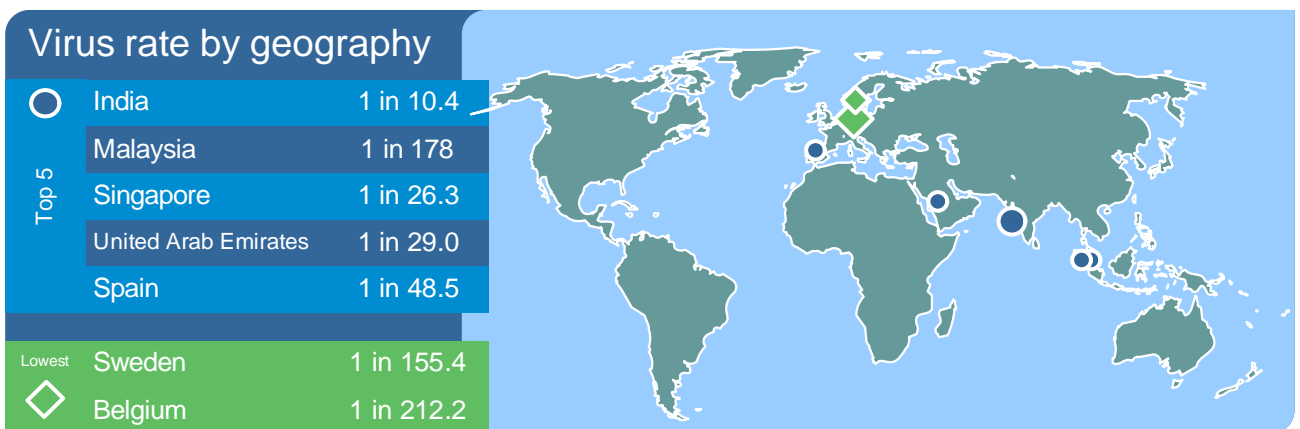
Geographical Breakdown: Based on Targeted Countries

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 June 2006.



Israel continues to dominate the spam charts in June, with an increase of 11.9% since May. The greatest rise however was seen in Ireland, which rose by 14.1% since the previous month.

The sharpest fall was observed in Spain, which is one of the lowest countries affected by spam in June.

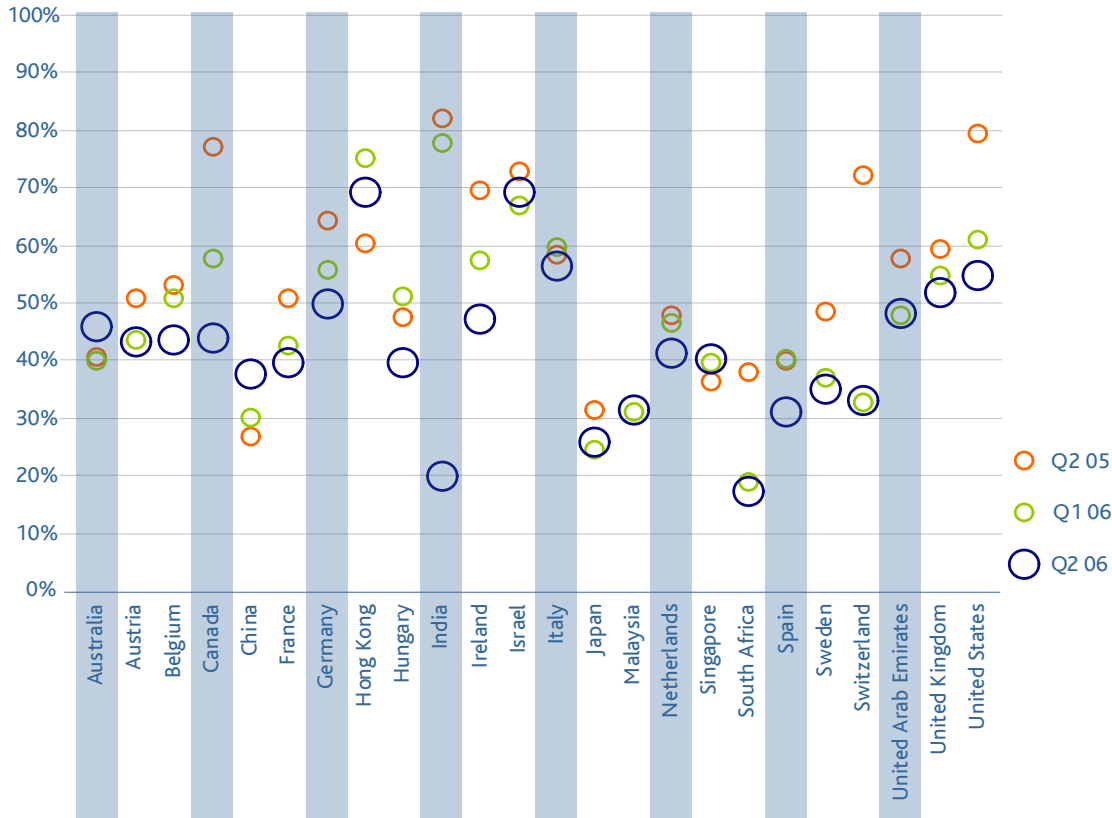


Again, India remains at the top of the virus chart for the fourth consecutive month since March, in the aftermath of the Nyxem.D outbreak in February. However, the good news is that virus traffic destined for the country fell by 0.9% from May.

The largest fall actually came in Germany (ranked 12th), and current home to the World Cup football competition taking place this month. The only country to suffer an increase in virus traffic during June was Japan, where attacks rose by 0.4% from the previous month.

Quarterly Review: The charts below have been specifically designed in order to highlight the interesting insights that may be gained by comparing quarter on quarter changes, but also the Q2 figures with the same period in 2005. Data for these charts may be found in the Appendix at the end of this report.

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

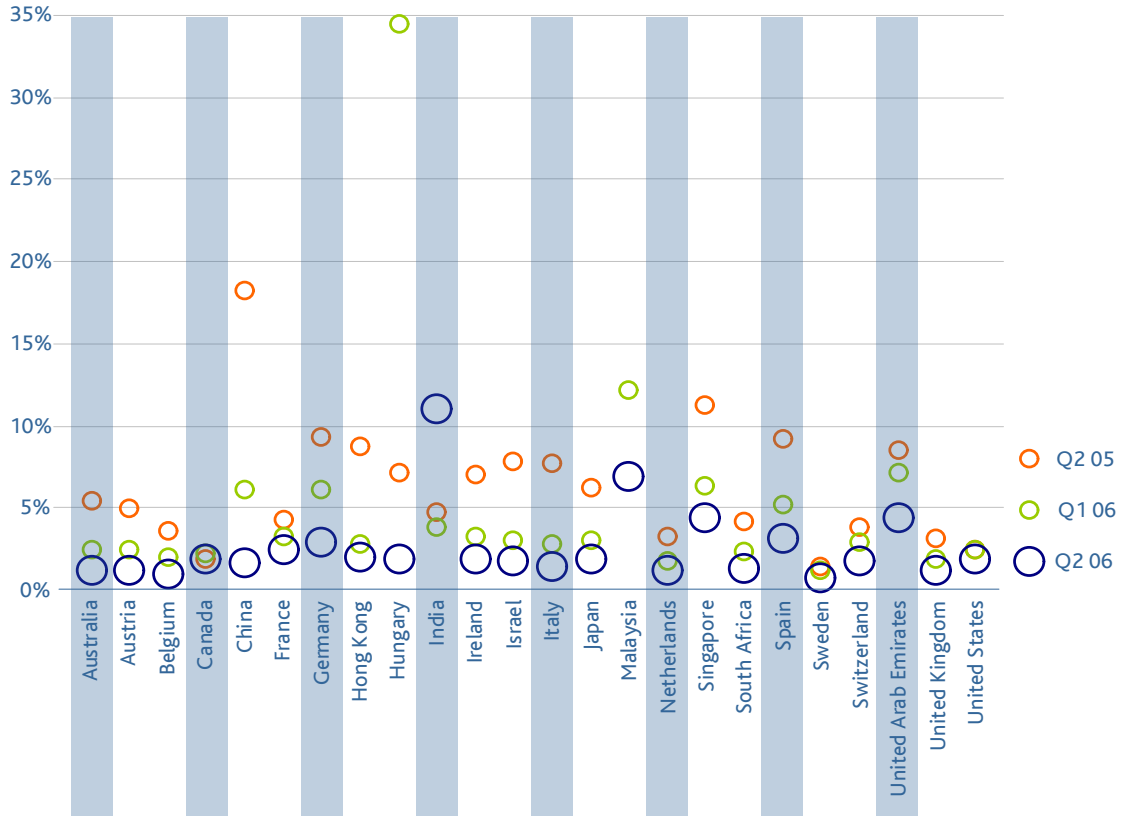


Also, for the first time, the top five countries on the receiving end of spam all experienced levels in excess of 50%. Some ISPs suggest that their customers never see much spam because they are able to filter it at the Internet-level. However, while these ISPs may be getting more effective at filtering, spammers are becoming more strident. "Filters make spamming harder, so spammers have to break the law to get a good delivery rate," suggested Amir Gans in a recent interview. Gans, the owner of a direct email marketing company based in Israel, is identified by SpamHaus as the number one spammer in Israel, and among the top spammers in the world.

Spam levels in India have plummeted in recent months, falling from 81.8% in Q2 2005, to 20.9% in June. Spam levels in Switzerland have fallen too, dropping by more than half in the last year, to a level of 32.9%.

In contrast, spam in China continues to rise despite the recent introduction of anti-spam legislation. The Internet Society of China (ISC) earlier revealed that spam is costing China an estimated \$756million (6.069-bn Chinese Yuan) every year.

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



Although the virus rate in India continues to rise in the wake of Nyxem.D, virus traffic in China has diminished significantly over the last 12 months - the country had been plagued with virus problems for a number of years.

A survey conducted in 2004 by the Ministry of Public Security of China (MPS) revealed that nearly 87.9% of the country's computer users had been infected by malware. This month the MPS is planning a much anticipated month-long follow-up investigation into the current state of China's Internet security issues arising from viruses, zombies and worms.

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 June 2006.

Spam rate by vertical			Virus rate by vertical		
Top 5	Chem/Pharm	72.5%	Top 5	Business Support Services	1 in 11.4
	Business Support Services	69.3%		Wholesale	1 in 26.8
	Recreation	68.0%		Manufacturing	1 in 57.3
	Education	65.2%		Non-Profit	1 in 64.1
	Manufacturing	62.1%		Education	1 in 68.7
Lowest	Mineral/Fuel	44.8%	Lowest	Chem/Pharm	1 in 198.0
	Gov/Public Sector	39.7%		Telcoms	1 in 278.5

The Chemical and Pharmaceutical sector remains dominant at the top of the spam chart for the second month in a row. With an increase of 11.1% in spam levels since May 2006, it received the greatest increase in spam observed across all sectors.

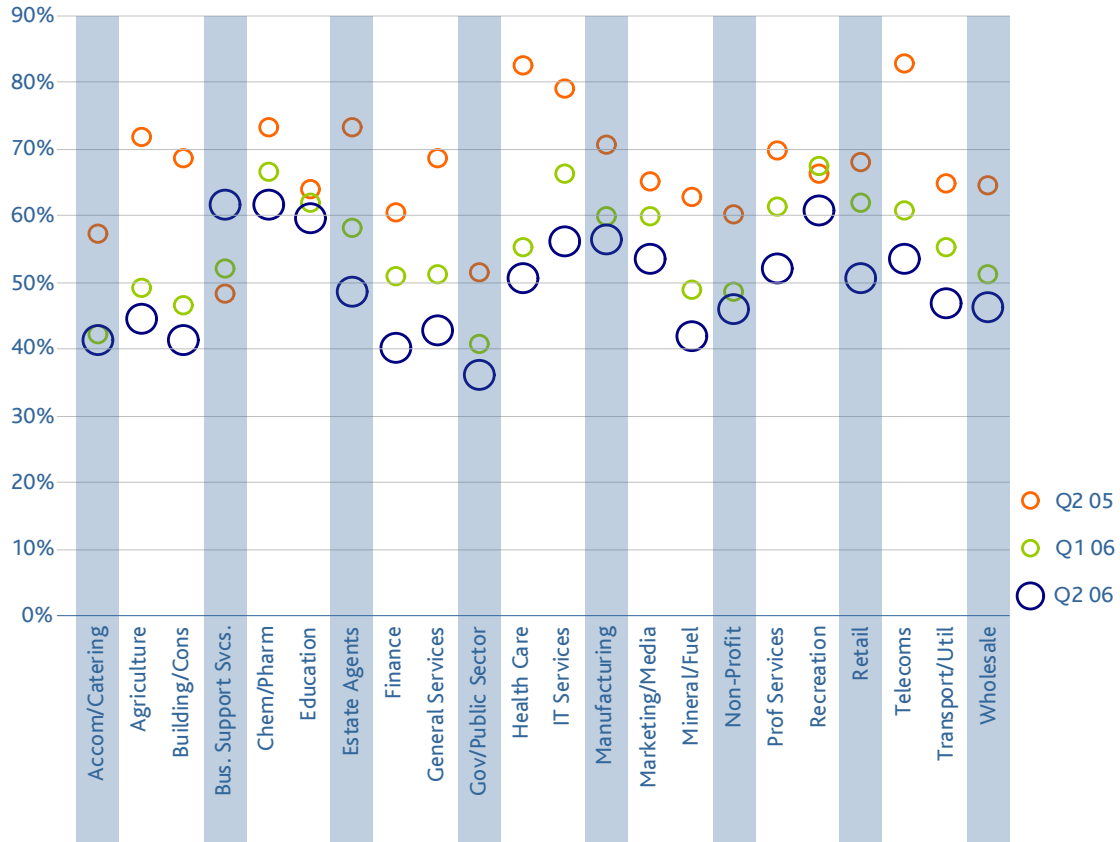
The greatest fall, or indeed the only fall, was in the spam destined for the Public Sector, which decreased by only 0.3% since the previous month.

Business Support Services is at the top of the virus chart in June, with the greatest increase in malicious email traffic across all sectors, and in fact, the only vertical to see an increase in virus traffic this month at all. Virus traffic destined for the Business Support Services vertical increased by 7.8% since May.

The largest fall was observed in the Education sector, which saw virus laden emails decrease by 1.5% when compared with the previous month.

Quarterly Review: The following charts highlight the interesting insights that may be gained by comparing quarter on quarter changes, as well comparing the Q2 figures with the same period in 2005.

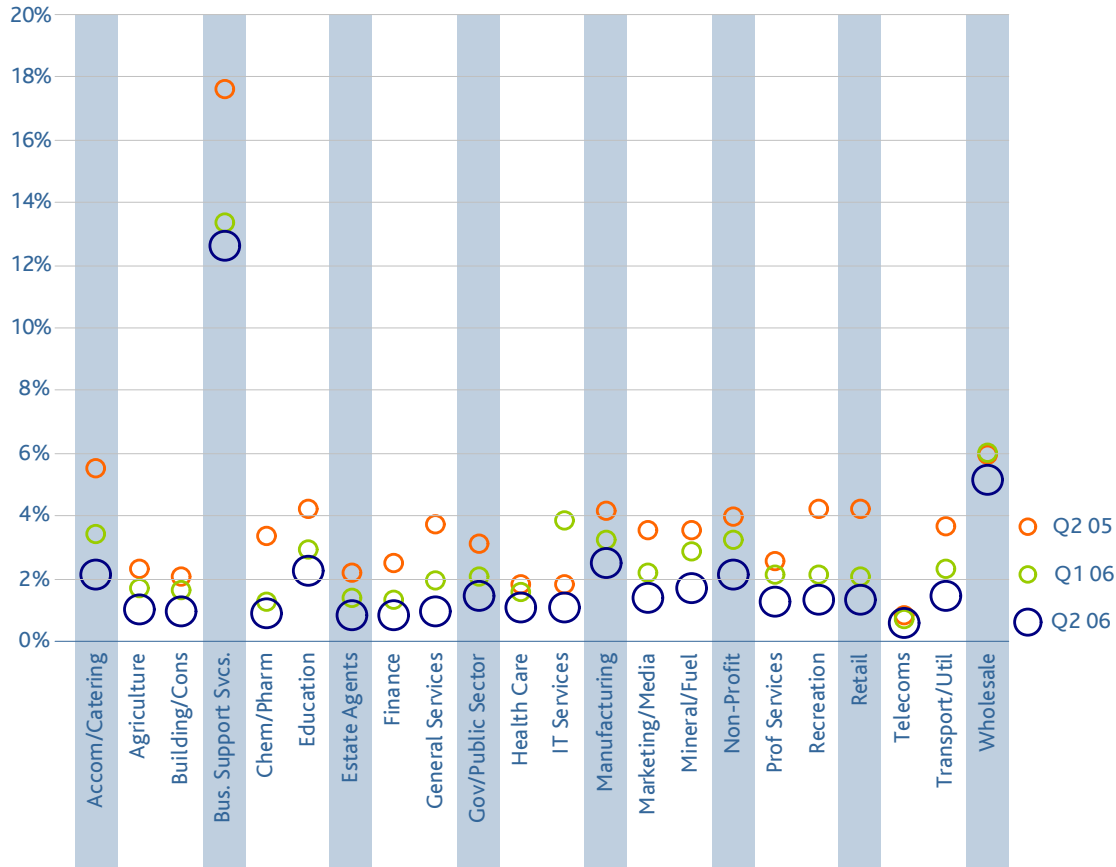
Spam Rate by Vertical (2006 Q1, Q2 and 2005 Q2)



Spam levels for the Business Support Services vertical continues to rise. Social networking tools have been cited as contributing factors as recruitment agencies rush to build virtual contact networks online.

Many professional tools such as Plaxo and LinkedIn also integrate their online networks with the users' Outlook contacts, automatically keeping them updated on any changes. This also means that should anyone in your virtual community become infected by spyware capable of tapping into this rich supply of email contacts, they will be guaranteed an accurate list of email addresses which they can spam.

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



As all businesses which rely on Microsoft Outlook and use Personal Storage folders (or PST files) to secure data offline know only too well, it is a relatively easy task to gain access to a supposedly encrypted email archive. Early waves of virus outbreaks that spread via email would use the address book of the recipient to further propagate to other users. No consideration was given for the potential value of this information in the early days, as it was used solely as a means to spread the virus.

Now, with access to local PST files and a rich harvest of accurate email addresses refreshed by the social networking environment, the same spyware code controlling the bot will also be used to not only profile the victim, but most of the people the victim corresponds with on a regular basis.

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 June, an average of 4.5% 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 June, an average of 14.9% 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 June would otherwise account for around 87% of global email traffic, an increase of 3.6% on the previous month.

Region	SMTP Validation (botnet sources)	User Validation (directory attacks)
USA	4.9%	14.9%
UK	3.8%	13.8%
Europe	4.2%	15.6%
Asia Pacific	7.6%	18.6%
Worldwide	4.5%	14.9%

Effects of Connection Management Techniques

MessageLabs is a leading provider of integrated messaging and web security services, with over 14,000 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 and 2005 Q2)

Spam Rate by Geography	Q2 05	Q1 06	Q2 06
Australia	40.3%	39.7%	45.7%
Austria	50.6%	43.6%	43.0%
Belgium	52.9%	50.6%	43.4%
Canada	77.1%	57.7%	43.7%
China	26.8%	30.0%	37.5%
France	50.5%	42.4%	39.4%
Germany	64.0%	55.5%	49.8%
Hong Kong	60.2%	75.1%	69.2%
Hungary	47.5%	50.9%	39.4%
India	81.8%	77.7%	19.7%
Ireland	69.3%	57.3%	47.1%
Israel	72.8%	66.7%	69.1%
Italy	58.2%	59.5%	56.1%
Japan	31.1%	24.3%	25.8%
Malaysia	0.0%	31.0%	31.3%
Netherlands	47.7%	46.5%	41.0%
Singapore	36.1%	39.5%	40.0%
South Africa	37.8%	18.8%	17.1%
Spain	39.9%	40.3%	31.0%
Sweden	48.3%	36.9%	35.0%
Switzerland	72.1%	32.5%	32.9%
United Arab Emirates	57.4%	47.6%	47.9%
United Kingdom	59.2%	54.5%	51.6%
United States	79.4%	61.0%	54.7%

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

Virus Rate by Geography	Q2 05	Q1 06	Q2 06
Australia	5.39%	2.35%	1.09%
Austria	4.87%	2.43%	1.16%
Belgium	3.55%	1.94%	0.94%
Canada	1.80%	2.13%	1.83%
China	18.13%	6.12%	1.65%
France	4.25%	3.18%	2.37%
Germany	9.23%	6.06%	2.86%
Hong Kong	8.74%	2.75%	1.95%
Hungary	7.09%	34.46%	1.88%
India	4.70%	3.83%	11.00%
Ireland	6.93%	3.24%	1.83%
Israel	7.83%	3.01%	1.66%
Italy	7.65%	2.71%	1.41%
Japan	6.22%	3.01%	1.82%
Malaysia	N/A	12.13%	6.91%
Netherlands	3.26%	1.76%	1.20%
Singapore	11.19%	6.33%	4.30%
South Africa	4.06%	2.31%	1.31%
Spain	9.17%	5.10%	3.12%
Sweden	1.40%	1.17%	0.71%
Switzerland	3.80%	2.82%	1.75%
United Arab Emirates	8.43%	7.14%	4.39%
United Kingdom	3.05%	1.81%	1.16%
United States	2.42%	2.40%	1.84%

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

Spam Rate by Vertical	Q2 05	Q1 06	Q2 06
Accom/Catering	57.3%	42.1%	41.3%
Agriculture	71.7%	49.2%	44.4%
Building/Cons	68.5%	46.5%	41.3%
Bus. Support Svcs.	48.3%	52.0%	61.7%
Chem/Pharm	73.2%	66.5%	61.6%
Education	63.9%	61.8%	59.5%
Estate Agents	73.2%	58.1%	48.4%
Finance	60.3%	50.8%	40.1%
General Services	68.6%	51.1%	42.7%
Gov/Public Sector	51.3%	40.7%	36.0%
Health Care	82.3%	55.2%	50.5%
IT Services	78.9%	66.1%	56.0%
Manufacturing	70.7%	59.8%	56.4%
Marketing/Media	65.1%	59.9%	53.3%
Mineral/Fuel	62.8%	48.7%	41.7%
Non-Profit	60.0%	48.6%	45.9%
Prof Services	69.6%	61.2%	52.0%
Recreation	66.3%	67.2%	60.7%
Retail	67.9%	61.8%	50.4%
Telecoms	82.7%	60.6%	53.4%
Transport/Util	64.6%	55.2%	46.7%
Wholesale	64.5%	51.2%	46.1%

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

Virus Rate by Vertical	Q2 05	Q1 06	Q2 06
Accom/Catering	5.48%	3.38%	2.10%
Agriculture	2.25%	1.67%	0.99%
Building/Cons	2.03%	1.63%	0.95%
Bus. Support Svcs.	17.58%	13.32%	12.61%
Chem/Pharm	3.36%	1.24%	0.89%
Education	4.17%	2.90%	2.20%
Estate Agents	2.18%	1.35%	0.82%
Finance	2.44%	1.32%	0.81%
General Services	3.68%	1.91%	0.92%
Gov/Public Sector	3.11%	2.05%	1.43%
Health Care	1.79%	1.52%	1.04%
IT Services	1.81%	3.84%	1.05%
Manufacturing	4.11%	3.19%	2.50%
Marketing/Media	3.53%	2.16%	1.35%
Mineral/Fuel	3.54%	2.85%	1.69%
Non-Profit	3.93%	3.18%	2.12%
Prof Services	2.54%	2.08%	1.23%
Recreation	4.19%	2.11%	1.28%
Retail	4.19%	2.04%	1.30%
Telecoms	0.80%	0.71%	0.53%
Transport/Util	3.64%	2.25%	1.42%
Wholesale	5.92%	6.01%	5.11%