



## MessageLabs Intelligence: July 2006

### Introduction

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

Top line results of this report include:

*Spam – 62.7% in July (a decrease of 2.1% since June)*

*Viruses – One in 96.6 emails in July contained malware (an increase of 0.05% since June)*

*Phishing – One in 459.8 emails comprised a phishing attack (an increase of 0.03% since June)*

Although overall threat levels remain stable when compared with the previous month, new scams abusing mobile text messaging and online social networking sites have come to the fore as the new “smarter” spam attacks. Exploitation through social engineering and targeted profiling of networking sites such as MySpace have been widely reported, and these threats continue to evolve as the convergence of these attacks continues. AOL’s Instant Messenger service was targeted for an attack earlier this month with messages spreading through the network which contained links to malicious botnet code, including spyware and other adware. IM is increasingly being used in this way, as messages from contacts in a buddy list are often considered more trustworthy and okay to open, however clicking on a malicious link in such a message can be very dangerous indeed.

Phishing attacks too have become much smarter, with Google’s Gmail becoming one of the latest targets, but the banking industry will be more worried by suggestions that two-factor authentication may be rendered useless. One particularly sophisticated phishing site demonstrated this point when it was uncovered that it could validate and make use of the one-time password credentials live, in real-time, as the user entered their details into the phishing site. These one-time passwords are typically generated on request by a security device issued by the bank; for example using a large number that changes every minute and is entered alongside the traditional username and password on the website. Although such attacks are still rare, it is likely that they will increase as the criminals attempt to remain one step ahead of the system, and more banks come online using similar two-factor devices.

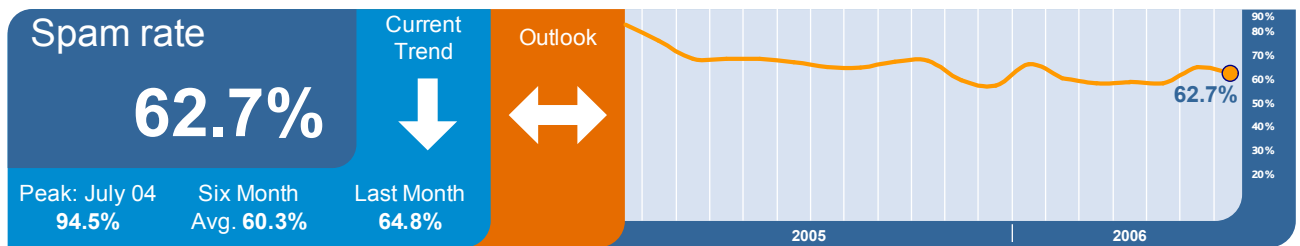
VoIP (Voice over IP) has been linked to the latest type of phishing attack, bizarrely dubbed “vishing”, or “voishing.” The victim receives an automated telephone call informing them that their credit card has been used illegally, and that they should dial a fake 1-800 number confirming their details. The latest twist however is that using VoIP, it is relatively easy for the caller to spoof the telephone number of the credit card company. Such impersonal calls should immediately be treated with caution, but as with more traditional forms of social engineering and confidence deceptions it is very difficult to safeguard against them as they often take place offline. With so many VoIP providers vying for market domination at the moment, call costs are relatively low, making such scams an attractive proposition.

Following on from last month’s report on the increasing use of low-level targeted attacks using “zero-day” exploits, MessageLabs reported only a few attacks using Microsoft PowerPoint, however in July this number increased from the beginning of the month to around the 11th July, when Microsoft issued 12 patches for its Office productivity suite, although the PowerPoint vulnerability remains unpatched at the time of writing. Microsoft Office remains the preferred target for these targeted attacks, some of which even played on recent events in the Middle East as a lure to open the attachment. Criminals are now employing the same techniques that are used by software quality and software security testers to discover the latest application crashes and to further investigate new potential vulnerabilities.

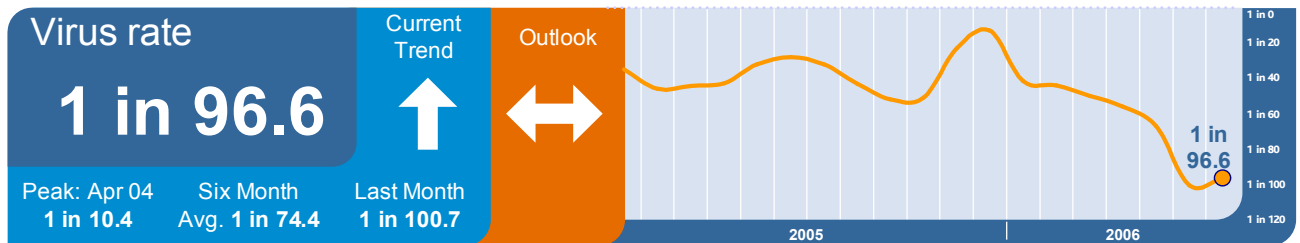
### Global Trends & Content Analysis

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.

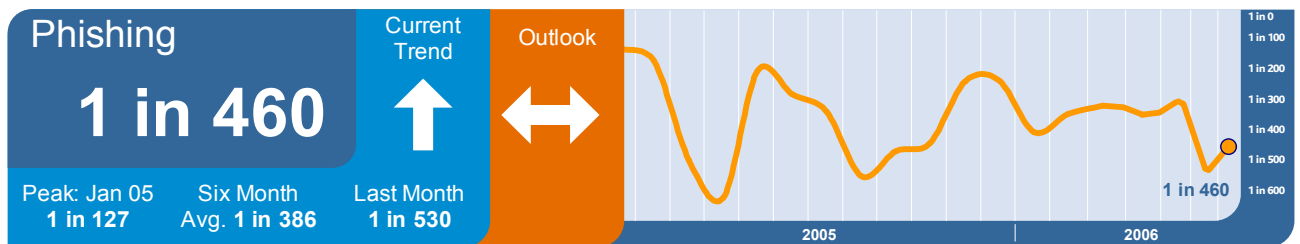
**Skeptic™ Anti-Spam Protection:** In July 2006, the global ratio of spam in email traffic from new and unknown bad sources, for which the recipient addresses were deemed valid, was 62.7% (1 in 1.59 emails), a decrease of 2.1% on the previous month.



**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 96.6 emails (1.04%) in July, an increase of 0.05% since June.



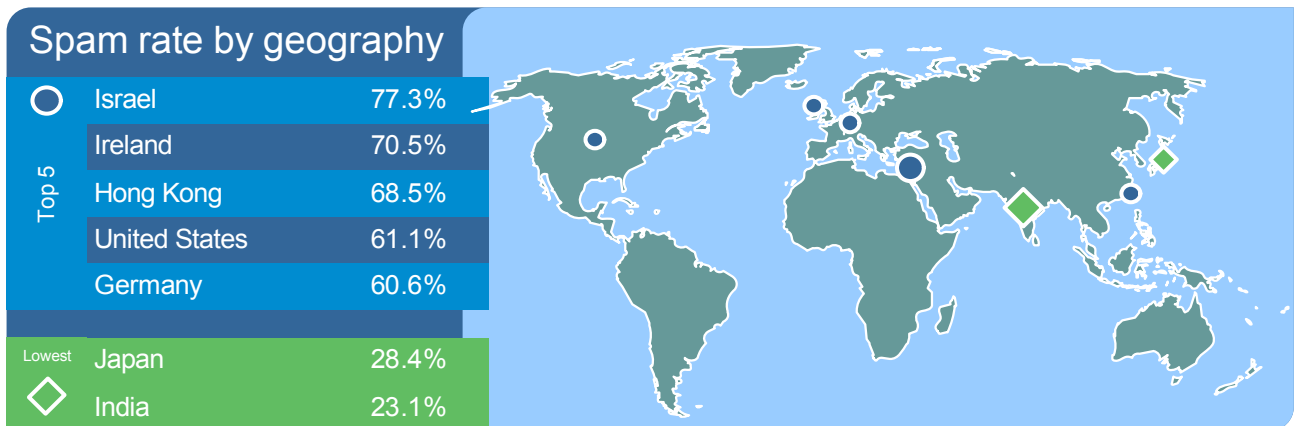
**Phishing:** July showed an increase of 0.03% in the proportion of phishing attacks compared with the previous month. One in 459.8 (0.22%) emails comprised some form of phishing attack.



When judged as a proportion of all email-borne threats including viruses and trojans, the proportion of phishing emails has risen by 2%, now accounting for 21% of all malicious emails intercepted by MessageLabs in July. The same figure for July 2005 was 9.6%.

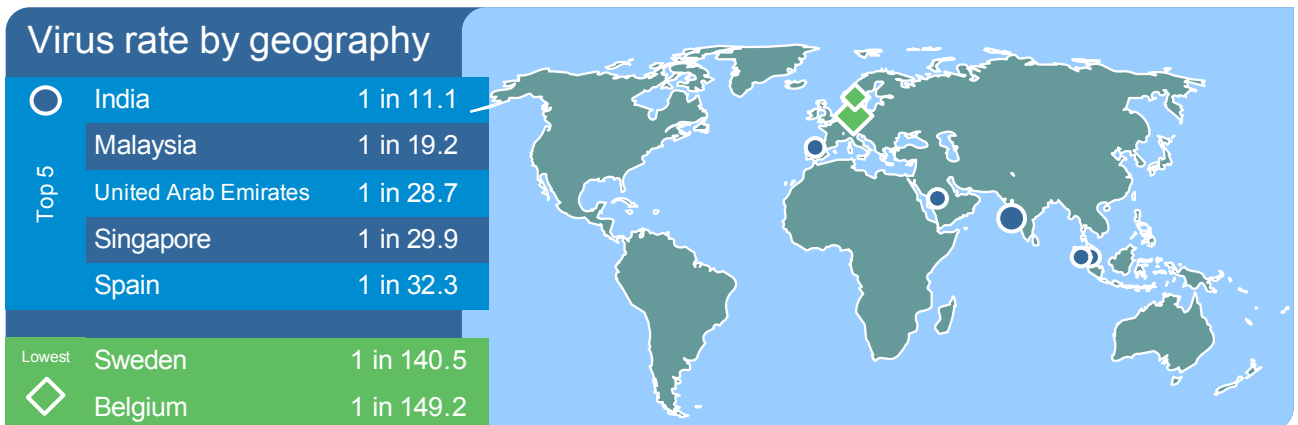
## Geographical Breakdown: Based on Targeted Countries

**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 July 2006.



In contrast to last month, Spain bore the greatest rise in spam this month, although positioned 14th in the chart and not shown here, spam levels increased by 21.1% to 45.9%. Spam levels in Ireland continued to rise by 11.1% to 70.5%, however, Israel is still targeted with the greatest proportion of spam, increasing by a further 1.4% since the previous month.

The largest drop occurred in Australia, where spam levels diminished by 3.2% to 48.8%.



India continues to bear the brunt of virus attacks in July, although the level dropped by 0.6% to 9%, where 1 in every 11.1 emails contained a virus. 0.6% represented the sharpest fall across all geographies since the previous month.

The sharpest increase was in Germany (positioned 6th), where 1 in 36.5 emails contained a virus, or 2.7%, rising by 1.4% since June.

## 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 July 2006.

Spam rate by vertical			Virus rate by vertical		
Top 5	Education	67.0%	Business Support Services	1 in 12.0	
	Recreation	67.0%	Wholesale	1 in 27.2	
	Manufacturing	63.9%	Accom/Catering	1 in 56.5	
	Telecoms	63.8%	Manufacturing	1 in 60.8	
	Chem/Pharm	62.7%	Non-Profit	1 in 64.6	
Lowest	General Services	43.0%	IT Services	1 in 163.1	
	Gov/Public Sector	36.3%	Telecoms	1 in 238.9	

Spam now accounts for 67% of email intended for the both the Education and Recreation sectors. Education rose by 1.8%, whilst Recreation fell by 1% since the previous month.

The largest increase in spam volumes across all sectors was in the Mineral/Fuel vertical, which was one of the lowest in June, but increased by 9.8% to 54.5%, moving into 12th position overall. In contrast, spam destined for the Chemical/Pharmaceutical sector fell by 9.8% to 62.7%, representing the largest fall in July across all sectors.

Spam targeted at the Telecoms industry rose by 5.5% in July, to 63.8%.

Virus traffic targeted at the Business Support Sector fell by 0.4%, the largest fall across all sectors, to 8.4% or 1 in 12 emails which contained a virus. The sharpest increase was in the Accommodation/Catering sector, which rose by 0.5% to 1.8% or 1 in 56.5 emails that contained a virus.

### 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 July, an average of 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 July, an average of 10.2% 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 July would otherwise account for around 86.8% of global email traffic, a decrease of 0.9% on the previous month.

Region	SMTP Validation (botnet sources)	User Validation (directory attacks)
USA	5.8%	9.8%
UK	4.1%	11.1%
Europe	4.2%	10.1%
Asia Pacific	6.5%	9.1%
<b>Worldwide</b>	<b>5.0%</b>	<b>10.2%</b>

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

For further information on MessageLabs Intelligence, please visit [www.messagelabs.com/intelligence](http://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 (July 2006)

Spam Rate by Geography	July 06	June 06	Change
Israel	77.3%	75.9%	1.4%
Ireland	70.5%	59.4%	11.1%
Hong Kong	68.5%	70.1%	-1.6%
United States	61.1%	58.6%	2.5%
Germany	60.6%	53.3%	7.3%
United Arab Emirates	60.1%	52.8%	7.3%
United Kingdom	56.3%	58.6%	-2.3%
Austria	56.2%	48.6%	7.6%
France	52.0%	45.2%	6.8%
Sweden	51.0%	38.5%	12.5%
Canada	49.9%	44.4%	5.5%
Netherlands	49.7%	43.8%	5.9%
Australia	48.8%	52.0%	-3.2%
Spain	45.9%	24.8%	21.1%
Singapore	45.4%	45.7%	-0.3%
Belgium	44.1%	37.0%	7.1%
Switzerland	37.4%	36.5%	0.9%
Malaysia	36.3%	33.3%	3.0%
Japan	28.4%	27.4%	1.0%
India	23.1%	20.9%	2.2%

**Appendix II: Virus Rate by Geography (July 2006)**

Virus Rate by Geography	July 06	June 06	Change
India	1 in 11.1 (9.0%)	1 in 10.4 (9.6%)	-0.6%
Malaysia	1 in 19.2 (5.2%)	1 in 17.8 (5.6%)	-0.4%
United Arab Emirates	1 in 28.7 (3.5%)	1 in 29.0 (3.5%)	0.1%
Singapore	1 in 29.9 (3.3%)	1 in 26.3 (3.8%)	-0.5%
Spain	1 in 32.3 (3.1%)	1 in 48.5 (2.1%)	1.0%
Germany	1 in 36.5 (2.7%)	1 in 72.3 (1.4%)	1.3%
France	1 in 43.9 (2.3%)	1 in 55.6 (1.8%)	0.5%
Hong Kong	1 in 48.9 (2.0%)	1 in 62.6 (1.6%)	0.4%
Japan	1 in 56.4 (1.8%)	1 in 53.8 (1.9%)	-0.1%
Ireland	1 in 67.0 (1.5%)	1 in 65.8 (1.5%)	0.0%
Switzerland	1 in 73.1 (1.4%)	1 in 71.5 (1.4%)	0.0%
United States	1 in 75.3 (1.3%)	1 in 74.1 (1.3%)	0.0%
Austria	1 in 95.6 (1.0%)	1 in 112.1 (0.9%)	0.1%
Netherlands	1 in 100.3 (1.0%)	1 in 115.0 (0.9%)	0.1%
Israel	1 in 108.1 (0.9%)	1 in 99.4 (1.0%)	-0.1%
Canada	1 in 108.8 (0.9%)	1 in 68.0 (1.5%)	-0.6%
Australia	1 in 127.6 (0.8%)	1 in 116.8 (0.9%)	-0.1%
United Kingdom	1 in 135.1 (0.7%)	1 in 132.9 (0.8%)	-0.1%
Sweden	1 in 140.5 (0.7%)	1 in 155.4 (0.6%)	0.1%
Belgium	1 in 149.2 (0.7%)	1 in 212.2 (0.5%)	0.2%

**Appendix III: Spam Rate by Vertical (July 2006)**

<b>Spam Rate by Vertical</b>	<b>July 06</b>	<b>June 06</b>	<b>Change</b>
Education	67.0%	65.2%	1.8%
Recreation	67.0%	68.0%	-1.0%
Manufacturing	63.9%	62.1%	1.8%
Telecoms	63.8%	58.2%	5.6%
Chem/Pharm	62.7%	72.5%	-9.8%
Business Support Svcs	61.9%	47.2%	-7.4%
Marketing/Media	61.1%	58.8%	2.3%
Transport/Utility	60.7%	52.3%	8.4%
Professional Services	59.1%	58.1%	1.0%
IT Services	55.6%	60.7%	-5.1%
Non-Profit	55.0%	51.0%	4.0%
Mineral/Fuel	54.5%	44.8%	9.7%
Wholesale	54.5%	51.5%	3.0%
Retail	54.4%	52.2%	2.2%
Health Care	54.3%	55.0%	-0.7%
Accom/Catering	51.3%	47.9%	3.4%
Building/Cons	49.5%	47.2%	2.3%
Finance	48.9%	46.7%	2.2%
General Services	43.0%	47.8%	-4.8%
Gov/Public Sector	36.3%	39.7%	-3.4%

**Appendix IV: Virus Rate by Vertical (July 2006)**

<b>Virus Rate by Vertical</b>	<b>July 06</b>	<b>June 06</b>	<b>Change</b>
Business Support Svcs	1 in 12.0 (8.4%)	1 in 137.5 (0.7%)	7.6%
Wholesale	1 in 27.2 (3.7%)	1 in 26.8 (3.7%)	0.0%
Accom/Catering	1 in 56.5 (1.8%)	1 in 76.3 (1.3%)	0.5%
Manufacturing	1 in 60.8 (1.6%)	1 in 57.3 (1.7%)	-0.1%
Non-Profit	1 in 64.6 (1.5%)	1 in 64.1 (1.6%)	-0.1%
Education	1 in 71.1 (1.4%)	1 in 68.7 (1.5%)	-0.1%
Mineral/Fuel	1 in 72.6 (1.4%)	1 in 80.5 (1.2%)	0.2%
Building/Cons	1 in 93.5 (1.1%)	1 in 137.5 (0.7%)	0.4%
Retail	1 in 96.7 (1.0%)	1 in 96.9 (1.0%)	0.0%
Transport/Util	1 in 97.0 (1.0%)	1 in 94.0 (1.1%)	-0.1%
Recreation	1 in 104.1 (1.0%)	1 in 116.2 (0.9%)	0.1%
Gov/Public Sector	1 in 104.2 (1.0%)	1 in 99.5 (1.0%)	0.0%
Marketing/Media	1 in 106.2 (0.9%)	1 in 117.2 (0.9%)	0.0%
Prof Services	1 in 114.7 (0.9%)	1 in 128.7 (0.8%)	0.1%
Health Care	1 in 117.6 (0.9%)	1 in 138.5 (0.7%)	0.2%
Chem/Pharm	1 in 118.4 (0.8%)	1 in 198.0 (0.5%)	0.3%
Finance	1 in 120.4 (0.8%)	1 in 160.2 (0.6%)	0.2%
General Services	1 in 142.1 (0.7%)	1 in 167.5 (0.6%)	0.1%
IT Services	1 in 163.1 (0.6%)	1 in 156.4 (0.6%)	0.0%
Telecoms	1 in 238.9 (0.4%)	1 in 278.5 (0.4%)	0.0%