MessageLabs®

Be certain

MessageLabs Intelligence: August 2006

Introduction

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

Top line results of this report include:

Spam – 64.5% in August (an increase of 1.8% since July)
Viruses – One in 98.4 emails in August contained malware (a decrease of 0.02% since July)
Phishing – One in 321 emails comprised a phishing attack (an increase of 0.1% since July)

As virus traffic settles to around 1% of email traffic in August, there is a marked shift in activity away from distributing email borne viruses and towards creating more targeted phishing attacks. If these attacks are measured as a proportion of virus and trojan activity, the level has significantly risen and now account for almost one third of all threats, compared to one-fifth of all threats in July, further highlighting this shift. This is a clear indication that online criminals are further concentrating their activities in this area, perhaps seizing the opportunity before two-factor authentication becomes a more rigorous standard across the banking industry. The eagerly anticipated arrival of Microsoft Windows Vista in the new year is also expected to deliver greater levels of security to the desktop than is available currently. However, before then, we may also expect Internet Explorer version 7.0 to be launched, offering integrated anti-phishing technology which will help in the detection of new phishing websites, making it much harder for these scams to be perpetrated.

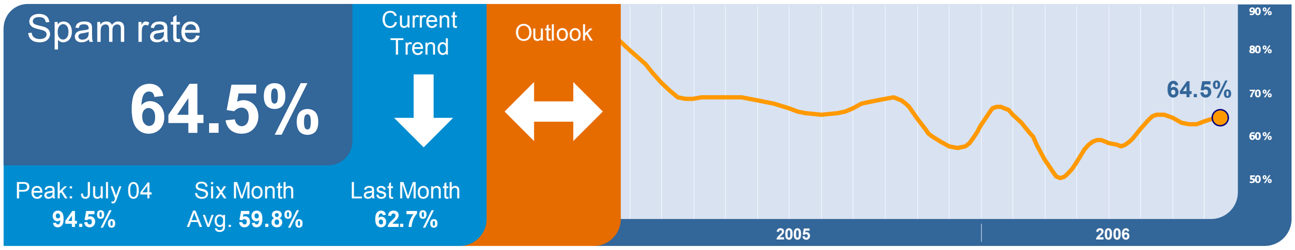
The threat landscape continues to converge as the web increasingly becomes targeted with more online attacks; not only are banks being targeted by sophisticated phishing scams, but other well-known brands including eBay and PayPal have been subjected to attacks via the web. More recently, popular social networking sites such as MySpace have come a barrage of pressure from cyber-criminals , and in order to address some of these issues, MySpace recently announced that they have now recruited a Chief Security Officer.

Earlier in August, Microsoft release another major security patch update, highlighting 9 “critical” and 3 “important” browser, Windows and Office-related vulnerabilities that could result in a computer becoming compromised. One vulnerability described in Microsoft’s MS06-040 security bulletin was already being exploited by two viruses, variants of W32/IRCBot, and both able to spread via AOL instant messenger as well as the MS06-040 exploit. The use of IM may dupe other users into downloading and executing the bot code via an external website, typically bypassing corporate firewalls within organizations that have no IM security, and then able to spread on the internal network once a machine has been successful compromised.

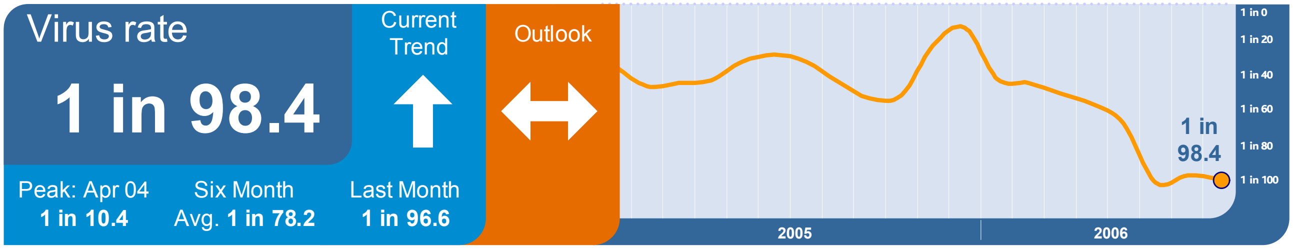
Furthermore, since August 16th , a well-known Russian spammer is also suspected of using the MS06-040 exploit technique to target unpatched corporate email servers in order to gain control and use them for distributing spam via Pro Mailer DMS, the notorious spam sending software. DMS is potentially more devastating than most spam-sending software since it is able to use the newer “spam cannon” technique that employs a powerful mail-merge of addresses with pre-prepared spam templates. This approach enables the spammer to maximize throughput and distribute millions of spam messages per hour through a single compromised computer, as mentioned in MessageLabs Intelligence Report May 2006.

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.

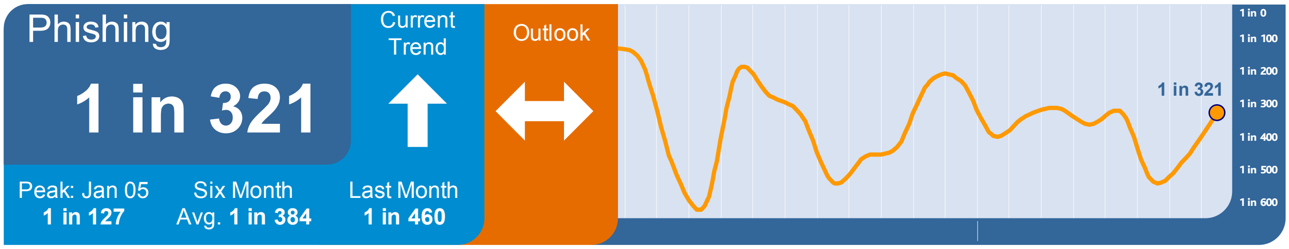
Skeptic™ Anti-Spam Protection: In August 2006, the global ratio of spam in email traffic from new and unknown bad sources, for which the recipient addresses were deemed valid, was 64.5% (1 in 1.55 emails), an increase of 1.8% on the previous month.



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 98.4 emails (1.02%) in August, an decrease of 0.02% since July.



Phishing: The proportion of phishing attacks for August was 1 in 321 emails (0.31%), an increase of 0.1% in the proportion of phishing attacks compared with the previous month.



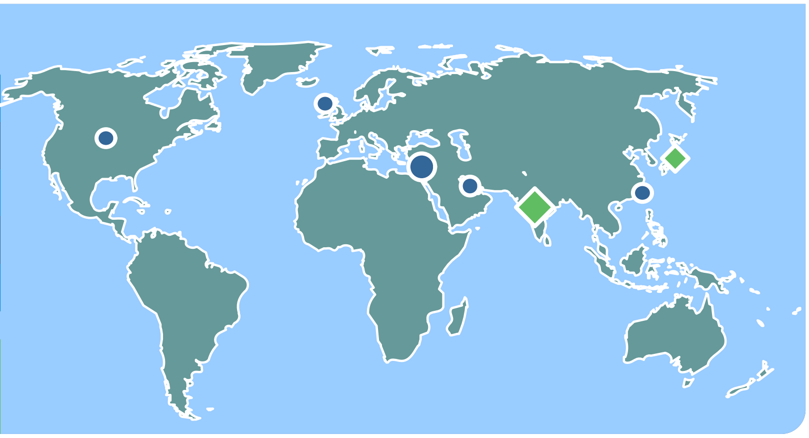
When judged as a proportion of all email-borne threats including viruses and trojans, the proportion of phishing emails has risen by 9.7% since July, now accounting for 30.7% of all malicious emails intercepted by MessageLabs in August.

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 August 2006.

Spam rate by geography

○ Top 5	Israel	78.0%
	Hong Kong	66.3%
	Ireland	62.5%
	United States	61.4%
	United Arab Emirates	58.3%
Lowest ◇	Japan	33.0%
	India	29.1%

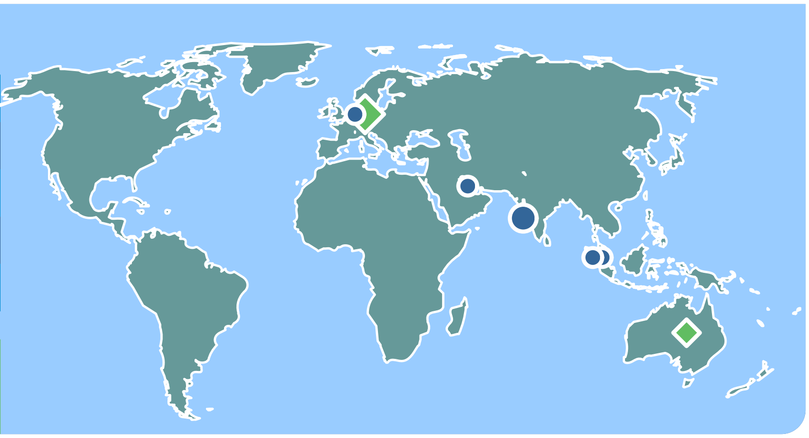


Of the Top 5 countries, the largest increase in spam destined for a particular country was observed in Israel, which was targeted 78% spam in August, an increase of 0.7% since July. The greatest drop was seen in Ireland, where spam fell by 8% to 62.5%.

Across all regions, the largest rise was in spam destined for Belgium, which increased by 9.5% to 53.6% in August. The greatest drop came in Sweden, where spam levels fell by 8.5% to 42.5%. The UK and Australia also achieved significant reductions in spam levels, dropping 7% and 6.9% respectively.

Virus rate by geography

○ Top 5	India	1 in 13.3
	Malaysia	1 in 21.2
	Germany	1 in 21.3
	United Arab Emirates	1 in 33.1
	Singapore	37.8
Lowest ◇	Australia	1 in 126.1
	Belgium	1 in 171.4



Across all regions the sharpest rise and fall for virus activity were both found in the Top 5 list of countries: The sharpest rise in virus activity came in Germany, where email virus traffic rose by 2% from 1 in 36.5 (2.7%) in July, to 1 in 21.3 (4.7%) in August, representing an almost two-fold increase month-on-month.

India remains the most targeted country for virus activity, despite benefiting from a 1.5% fall in virus traffic, from 1 in 11.1 (9.0%) in July to 1 in 13.3 (7.5%), representing the largest drop in August across all regions and the Top 5 countries.

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 August 2006.

Spam rate by vertical

Top 5	Education	68.2%
	Manufacturing	62.8%
	Recreation	61.8%
	Transport/Util	59.1%
	Wholesale	58.1%
Lowest	General Services	40.0%
	Gov/Public Sector	37.9%

Virus rate by vertical

Top 5	Business Support Services	1 in 14.5
	Wholesale	1 in 33.5
	Education	1 in 51.7
	Accom/Catering	1 in 58.3
	Non-Profit	1 in 66.2
Lowest	IT Services	1 in 159.1
	Telecoms	1 in 216.9

Of the Top 5 industry sectors, the Wholesale vertical bore the brunt of the largest increase of spam this month, rising by 3.6% to 58.1% in August, also representing the greatest increase across all sectors. The sharpest fall in the Top 5 came in the Recreation sector, which dropped by 5.2% to 61.8% in August. The largest fall against all sectors came in the Real Estate field with a 15.1 percent drop this month in spam levels, moving it from top of the table in July with 67 percent rate to 51.9 percent in August.

Of the Top 5 industry sectors, the Education sector saw the greatest increase in viruses spam this month, rising by 0.5% from 1 in 71.1 (1.4%) in July to 1 in 51.7 (1.9%) in August, also representing the greatest increase across all sectors.

Business Support Services remains the most targeted industry sector in August, despite witnessing the largest drop in virus activity in the Top 5 industry sectors, falling by 1.5% from 1 in 12.0 (8.3%) in July to 1 in 14.5 (6.9%) this month. Across all industry sectors, the sharpest decrease came in the Building and Construction sector, which fell by 7.4% from 1 in 12.0 (8.3%) in July to 1 in 113.3 (0.9%) in August.

Full details of geographical and industry analysis may be referenced in the Appendices accompanying this report.

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 August, an average of 4.8% 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 August, 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 August would otherwise account for around 84.9% of global email traffic, a decrease of 1.9% on the previous month.

	SMTP Validation	**User Validation**
Region	*(botnet sources)*	*(directory attacks)*
USA	5.00%	12.30%
UK	4.50%	11.90%
Europe	4.70%	10.90%
Asia Pacific	4.30%	10.70%
Worldwide	**4.80%**	**11.90%**

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 (August 2006)

Spam Rate by Geography	6-Aug	6-Jul	Change
Israel	78.00%	77.30%	0.70%
Hong Kong	66.30%	68.50%	-2.20%
Ireland	62.50%	70.50%	-8.00%
United States	61.40%	61.10%	0.30%
United Arab Emirates	58.30%	60.10%	-1.80%
Austria	58.00%	56.20%	1.80%
Germany	57.40%	60.60%	-3.20%
France	54.90%	52.00%	2.90%
Belgium	53.60%	44.10%	9.50%
Canada	51.70%	49.90%	1.80%
Netherlands	50.50%	49.70%	0.80%
United Kingdom	49.30%	56.30%	-7.00%
Singapore	46.20%	45.40%	0.80%
Spain	43.10%	45.90%	-2.80%
Sweden	42.50%	51.00%	-8.50%
Australia	41.90%	48.80%	-6.90%
Switzerland	41.30%	37.40%	3.90%
Malaysia	36.50%	36.30%	0.20%
Japan	33.00%	28.40%	4.60%
India	29.10%	23.10%	6.00%

Appendix II: Virus Rate by Geography (August 2006)

Virus Rate by Geography	6-Aug	6-Jul	Change
India	1 in 13.3 (7.5%)	1 in 11.1 (9.0%)	-1.50%
Malaysia	1 in 21.2 (4.7%)	1 in 19.2 (5.2%)	-0.50%
Germany	1 in 21.3 (4.7%)	1 in 36.5 (2.7%)	2.00%
United Arab Emirates	1 in 33.1 (3.0%)	1 in 28.7 (3.5%)	-0.50%
Singapore	1 in 37.8 (2.6%)	1 in 29.9 (3.3%)	-0.70%
Ireland	1 in 38.7 (2.6%)	1 in 67.0 (1.5%)	1.10%
Spain	1 in 39.4 (2.5%)	1 in 32.3 (3.1%)	-0.60%
France	1 in 39.6 (2.5%)	1 in 43.9 (2.3%)	0.20%
Hong Kong	1 in 55.2 (1.8%)	1 in 48.9 (2.0%)	-0.20%
Switzerland	1 in 69.5 (1.4%)	1 in 73.1 (1.4%)	0.00%
Japan	1 in 85.8 (1.2%)	1 in 56.4 (1.8%)	-0.60%
Austria	1 in 88.0 (1.1%)	1 in 95.6 (1.0%)	0.10%
Sweden	1 in 91.4 (1.1%)	1 in 140.5 (0.7%)	0.40%
United States	1 in 94.8 (1.1%)	1 in 75.3 (1.3%)	-0.20%
Netherlands	1 in 95.4 (1.0%)	1 in 100.3 (1.0%)	0.00%
United Kingdom	1 in 105.9 (0.9%)	1 in 135.1 (0.7%)	0.20%
Israel	1 in 107.6 (0.9%)	1 in 108.1 (0.9%)	0.00%
Canada	1 in 116.2 (0.9%)	1 in 108.8 (0.9%)	0.00%
Australia	1 in 126.1 (0.8%)	1 in 127.6 (0.8%)	0.00%
Belgium	1 in 171.4 (0.6%)	1 in 149.2 (0.7%)	-0.10%

Appendix III: Spam Rate by Vertical (August 2006)

Spam Rate by Vertical	6-Aug	6-Jul	Change
Education	68.20%	67.00%	1.20%
Manufacturing	62.80%	63.90%	-1.10%
Recreation	61.80%	67.00%	-5.20%
Transport/Util	59.10%	60.70%	-1.60%
Wholesale	58.10%	54.50%	3.60%
Telecoms	57.90%	63.80%	-5.90%
Chem/Pharm	57.80%	62.70%	-4.90%
Marketing/Media	56.20%	61.10%	-4.90%
Health Care	56.10%	54.30%	1.80%
Retail	56.00%	54.40%	1.60%
Prof Services	54.30%	59.10%	-4.80%
IT Services	53.30%	55.60%	-2.30%
Mineral/Fuel	52.90%	54.50%	-1.60%
Estate Agents	51.90%	67.00%	-15.10%
Non-Profit	51.10%	55.00%	-3.90%
Accom/Catering	50.60%	51.30%	-0.70%
Building/Cons	49.00%	49.50%	-0.50%
Finance	45.00%	48.90%	-3.90%
General Services	40.00%	43.00%	-3.00%
Gov/Public Sector	37.90%	36.30%	1.60%

Appendix IV: Virus Rate by Vertical (August 2006)

Virus Rate by Vertical	6-Aug	6-Jul	Change
Business Support Svcs	1 in 14.5 (6.9%)	1 in 12.0 (8.3%)	-1.40%
Wholesale	1 in 33.5 (3.0%)	1 in 27.2 (3.7%)	-0.70%
Education	1 in 51.7 (1.9%)	1 in 71.1 (1.4%)	0.50%
Accom/Catering	1 in 58.3 (1.7%)	1 in 56.5 (1.8%)	-0.10%
Non-Profit	1 in 66.2 (1.5%)	1 in 64.6 (1.5%)	0.00%
Manufacturing	1 in 70.5 (1.4%)	1 in 60.8 (1.6%)	-0.20%
Mineral/Fuel	1 in 76.0 (1.3%)	1 in 72.6 (1.4%)	-0.10%
Gov/Public Sector	1 in 84.8 (1.2%)	1 in 104.2 (1.0%)	0.20%
Marketing/Media	1 in 87.4 (1.1%)	1 in 106.2 (0.9%)	0.20%
Transport/Util	1 in 95.6 (1.0%)	1 in 97.0 (1.0%)	0.00%
Retail	1 in 104.9 (1.0%)	1 in 96.7 (1.0%)	0.00%
Chem/Pharm	1 in 107.8 (0.9%)	1 in 118.4 (0.8%)	0.10%
Recreation	1 in 109.4 (0.9%)	1 in 104.1 (1.0%)	-0.10%
Prof Services	1 in 112.1 (0.9%)	1 in 114.7 (0.9%)	0.00%
Building/Cons	1 in 113.3 (0.9%)	1 in 12.0 (8.3%)	-7.40%
General Services	1 in 122.1 (0.8%)	1 in 142.1 (0.7%)	0.10%
Finance	1 in 128.0 (0.8%)	1 in 120.4 (0.8%)	0.00%
Health Care	1 in 148.1 (0.7%)	1 in 117.6 (0.9%)	-0.20%
IT Services	1 in 159.1 (0.6%)	1 in 163.1 (0.6%)	0.00%
Telecoms	1 in 216.9 (0.5%)	1 in 238.9 (0.4%)	0.10%