MessageLabs®

Be certain

MessageLabs Intelligence: May 2006

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

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.

Over the last few months, it has become increasingly apparent that as the technological arms race escalates, SMEs are now more than ever being confronted with the same security threats as larger enterprises, however, as the threats become more sophisticated, smaller companies are finding it more difficult to keep pace and safeguard their information systems.

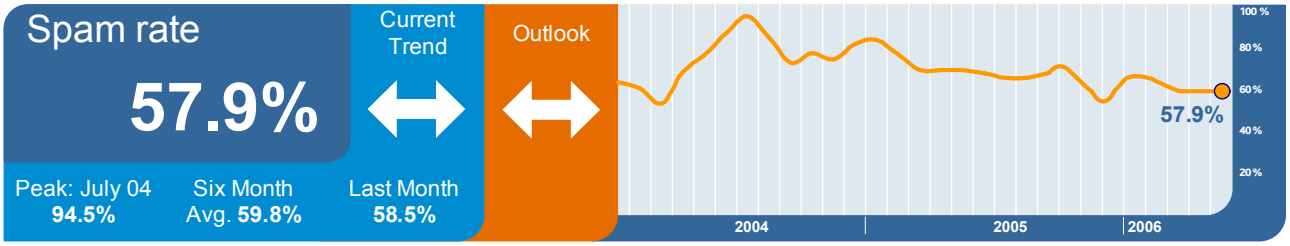
According to the latest Information Security Breaches Survey of 1,000 UK businesses and produced by the DTI and PricewaterhouseCoopers, nearly three times as many companies now have a security policy as did six years ago, and 98% of businesses have anti-virus software in place; 80% of which update their signatures every day. Although the number of companies infected has fallen, the average number of infections each company suffered rose to roughly one per day, with several businesses reporting hundreds of infections per day, with around a quarter of companies reporting a virus as their worst incident, causing major disruption.

According to the same report, 86% of the companies surveyed also filtered incoming email for spam. The report also noted that a quarter of UK businesses are not protected against spyware and 40% of businesses that allow instant messaging, have no controls in place over its use.

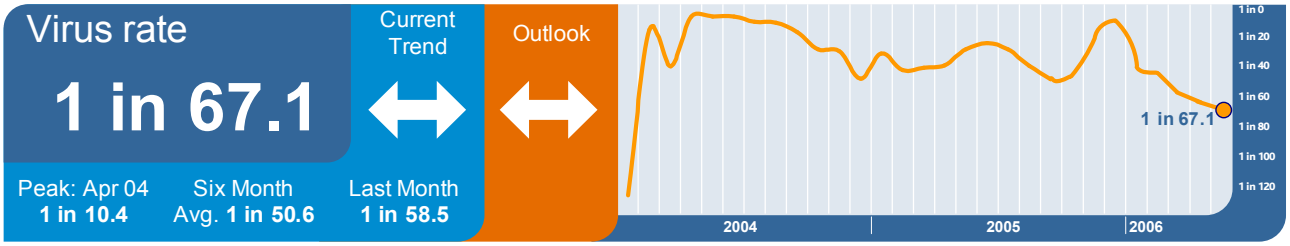
In recent months, new issues such as “Domain Kiting” (or “Disposable Domains”) and “Spam Cannons” have escalated to become much more of a serious threat than they were even a few months earlier. Disposable Domains was an issue first raised in the MessageLabs Intelligence 2005 End-of-Year report, but is now apparently being exploited by spammers via certain domain registrars using the controversial RFC 3915 “Domain Registry Grace Period Mapping for the Extensible Provisioning Protocol” loophole.

Spyware has become intrinsic to the means by which bot technology has further converged with viruses, trojans and spam – and the boundaries between them are almost impossible to distinguish. A traditional botnet may be likened with peas in a tube – by pushing one pea in, another pea pops-out at the other end – botnets provide this degree of anonymity, but are not often very scalable. However, the latest techniques use a mail-merge tactic that combines lists of harvested names and email addresses with email templates – all downloaded from a control server on demand – thus transforming the pea-shooters of old into a veritable “spam cannon” able to pump out millions of emails per hour using mass-mailing, mail-merge technology.

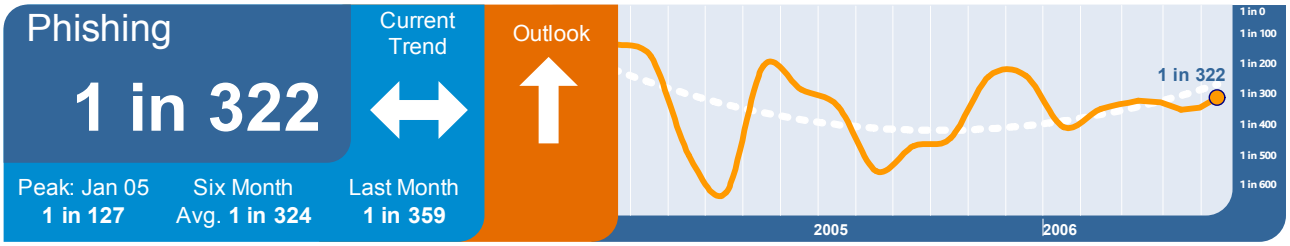
Skeptic™ Anti-Spam Protection: In May, the global ratio of spam in email traffic from new and unknown bad sources, for which the recipient addresses were deemed valid, was 57.9% (1 in 1.7), a decrease of 0.6% on the previous month.



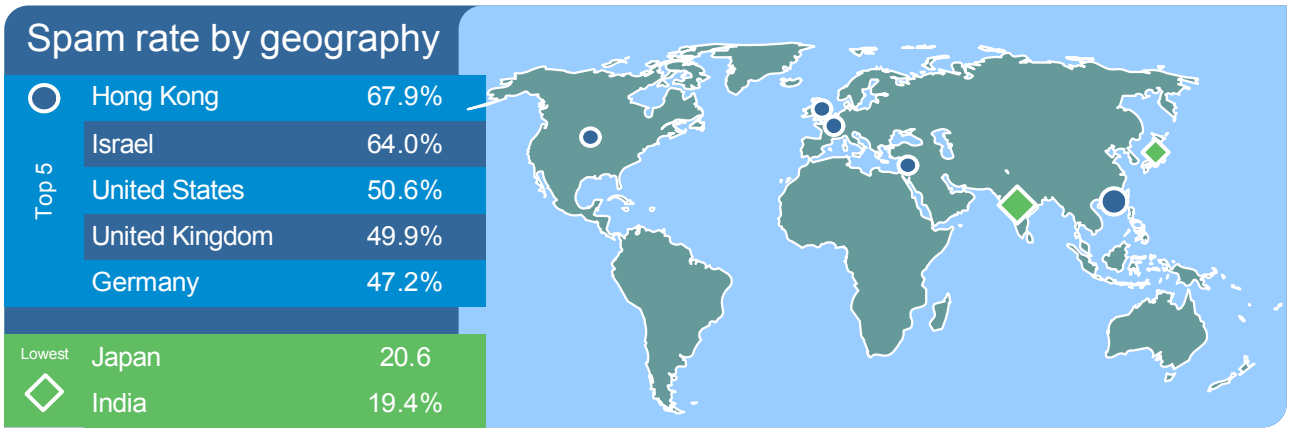
Skeptic™ Anti-Virus and Trojan Protection: The global ratio of email-borne viruses in email traffic from new and previously unknown bad sources destined for valid recipients, was 1 in 67.1 (1.5%) in May, a decrease of 0.3% since April.



Phishing: May showed an increase of 0.03% in the proportion of phishing attacks compared with the previous month. One in 322.8 (0.31%) emails was a phishing attack. The number of phishing attacks also increased by 5.2% as a proportion of all email-borne threats, now accounting for 20.8% of all malicious emails intercepted by MessageLabs in May.

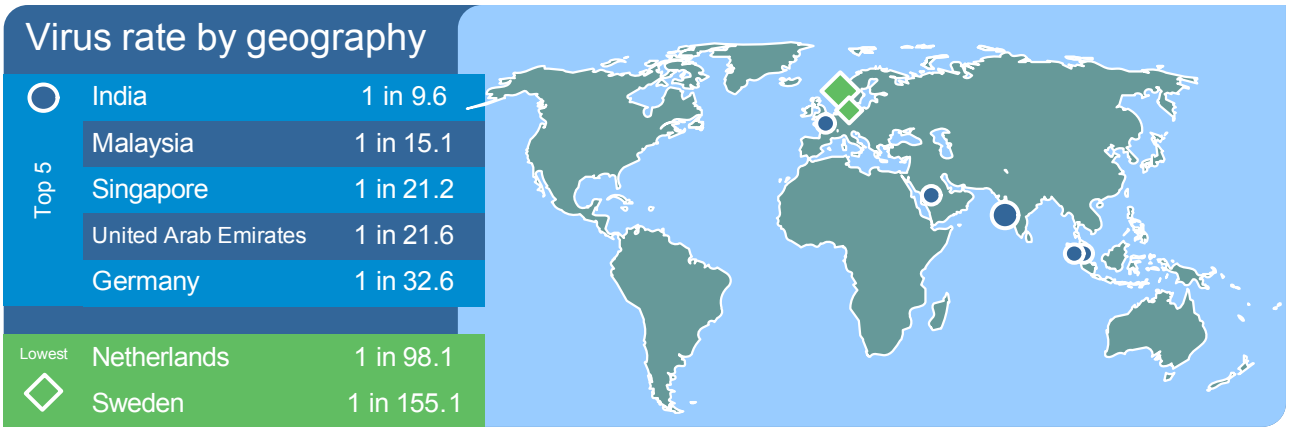


Geographical Breakdown: Based on Targeted Countries
By analyzing the geographical dispersal of email traffic where possible, MessageLabs compiles data that shows the impact and vulnerability rates of spam and viruses for specific countries. The charts below reflect impact and ratios for May 2006:



The country being on the receiving end of the greatest proportion of spam again is Hong Kong, dropping by only 1.4% on the previous month. The greatest increase was seen in Malaysia (ranked 18th in the list), where spam accounted for 20% of email volume last month, but now accounts for 31%. The highest drop was seen in Canada (ranked 11th in the list), which fell by 7.8% to 40.3%.

All of those in the top-5 decreased by an average of 2.1% compared with the April figures, with the exception of the UK, which bucked the trend with spam increasing by 2% on the previous month.



Again, India continues to suffer as the most profusely affected country in the virus chart, the proportion of virus laden emails decreasing by only 3.7% to 1 in 9.6, since April. The greatest increase in virus traffic was seen in Malaysia, where virus borne email traffic rose by 4.5% on the previous month to 1 in 15.1.

Vertical Industry Breakdown
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 May 2006:

Spam rate by vertical		
Top 5	Chem/Pharm	61.4%
	Business Support Services	61.3%
	Recreation	58.6%
	Education	57.9%
	IT Services	54.8%
Lowest	Accom/Catering	38.5%
	Finance	36.9%

Virus rate by vertical		
Top 5	Wholesale	1 in 21.5
	Education	1 in 33.7
	Manufacturing	1 in 39.9
	Accom/Catering	1 in 43.8
	Non-Profit	1 in 50.8
Lowest	Finance	1 in 135.7
	Telcoms	1 in 192.9

The vertical most affected by email spam is the Chemical & Pharmaceutical industry, with the greatest increase in the proportion of spam in email traffic from the previous month. Increasing by 4.5% to 61.4% in May, the Chemical & Pharmaceutical sector ranks at number one in May. The greatest drop was within the Wholesale sector (ranked 12th this month), which saw spam traffic falling by 9% to 43.6%.

The vertical most targeted in May, with 1 in 21.5 of email containing a virus, was the Wholesale sector. Even with a slight fall of only 1.3% when compared with the previous month, it still manages to take the top spot from Business Support Services (now ranked 15th), which bore the greatest fall of 17.4% to now 0.9% (1 in 106.6).

The Education sector witnessed the greatest rise in virus traffic, with 1 in 33.7 emails harboring a virus; this is an increase of 0.9% since April.

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 May, on average 6.1% 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 May, on average 10.8% 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 May would otherwise account for an average of 82.5% of global email traffic.

Region	SMTP Validation (botnet sources)	User Validation (directory attacks)
USA	7.30%	11.20%
UK	4.90%	10.10%
Europe	5.40%	10.00%
Asia Pacific	4.30%	15.40%
Worldwide	**6.10%**	**10.80%**

Effects of Connection Management Techniques

MessageLabs is the world's leading provider of email security and management services with more than 13,000 clients.

MessageLabs Intelligence is a respected source of data and analysis for email security issues, trends and statistics. MessageLabs provides a range of information on global email security threats based on live data feeds from its control towers around the world.

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.