MessageLabs Intelligence: March 2006

Introduction
Welcome to the March edition of the MessageLabs Intelligence monthly report. This report provides the latest threat trends for March 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.

Skeptic™ Anti-Spam Protection: In March, the global ratio of spam in email traffic from new and unknown bad sources, for which the recipient addresses were deemed valid, was 57.8% (1 in 1.7), a drop of 2.8% on the previous month. This would suggest that since the overall proportion of spam has not changed, botnet sizes have remained fairly stable.

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 59.1 (1.7%), a decrease of less than one percent from the previous month.

On average, MessageLabs detects around 10 “new” worms that are designed to spread bot programs each day. These worms are based on existing malicious code but have been obfuscated in an attempt to avoid detection by signature based anti-virus software.

Although the average size of a botnet hasn't changed significantly in recent months, the number of active botnets does continue to rise, as does the usage of botnets to install various 'Pay-Per-Install' adware applications. In March, new strains of the infamous Bagle worm were discovered which suggests a more sinister development in the creation of the Bagle botnets.

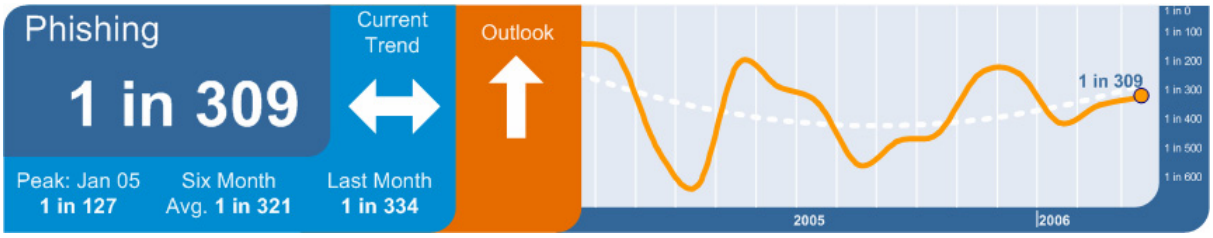
Like most bots, Bagle implements backdoor and proxy technology, through which access to the infected computer can be gained and spam can be relayed remotely. However, this strain tries to hide itself from the

operating system and security software using rootkit techniques by installing a kernel-mode device driver that hooks various system calls in order to conceal malicious files, processes and registry keys.

Most of these new Bagles would have been downloaded from compromised websites by machines already infected with previous Bagle variants, making it increasingly difficult for previous victims of the Bagle virus to have a clean computer.

Downloaders and other trojans continue to be the "malware of choice" at the moment, a tendency first observed in February. This is explained by major advances in technology for detecting mass-mailing malware, coupled with the desire to create an attractive market for trojans that remain invisible for longer, as opposed to those that draw attention to themselves by continually sending virus infected emails.

Phishing: March showed an increase of 0.02% in the proportion of phishing attacks compared with the previous month. One in 309.2 (0.32%) emails was a phishing attack. The number of phishing attacks has increased by 1.3% as a proportion of all email-borne threats, now accounting for 14.5% of all malicious emails intercepted by MessageLabs in March.



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 chart below reflects impacts and ratios for March 2006:

Spam rate by vertical

Top 5	Chem/Pharm	58.6%
	Recreation	57.2%
	Retail	55.7%
	Education	54.9%
	IT Services	54.0%
Lowest	Building/Constuction	40.1%
	Gov't/Public Sector	37.4%

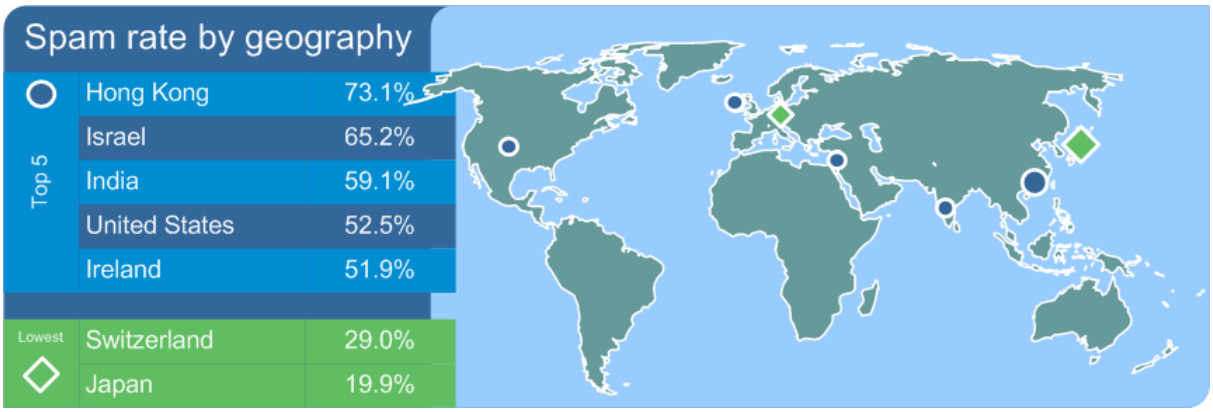
Virus rate by vertical

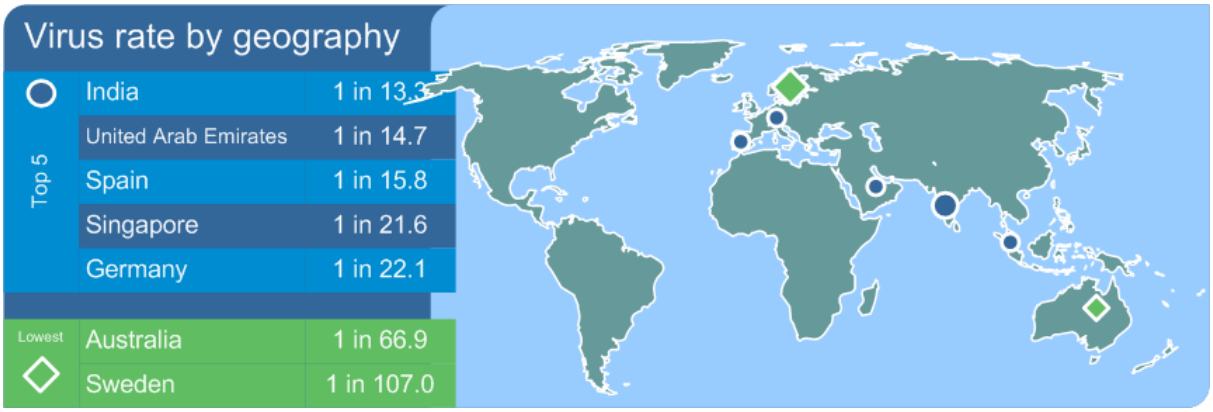
Top 5	Business Support Services	1 in 7.4
	Wholesale	1 in 14.1
	Non-Profit	1 in 32.8
	Education	1 in 32.9
	Manufacturing	1 in 34.4
Lowest	Finance	1 in 89.0
	Telcoms	1 in 143.4

Business Support Services continue to be plagued by virus traffic, as is often the case after a large outbreak, such at the Nyxem (aka MyWife) worm in January. This vertical includes businesses that provide office administration and support functions as well as human resourcing and recruitment agencies.

This is not unusual, since recruitment agencies in particular often suffer collateral damage from large outbreaks, since their email addresses regularly appear in people's address books, which may also be connected through online social networking tools.

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 specific to geographies. The chart below reflects impact and ratios for March 2006:





India continues to be in the thrall of the Nyxem worm, as clean-up efforts after the January attack continue. Internet connectivity in the region is growing as privatization has reduced costs, although this still tends to be concentrated around the major cities.

The internet provides an efficient communications tool for businesses in the region, a gateway to the overseas market, however this does come at a price. With relatively new exposure to the internet and with many ISPs still developing their infrastructure, security considerations are not as advanced as they should be which is reflected in the high virus and spam figures.

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 March, on average 5.5% 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 March, on average 12.3% 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 March would otherwise account for an average of 82.5% of global email traffic.

Region	SMTP Validation (botnet sources)	User Validation (directory attacks)
USA	5.3%	13.0%
UK	5.1%	9.0%
Europe	5.4%	13.2%
Asia Pacific	8.4%	20.6%
Worldwide	**5.5%**	**12.3%**

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.