



MessageLabs Intelligence: January 2006

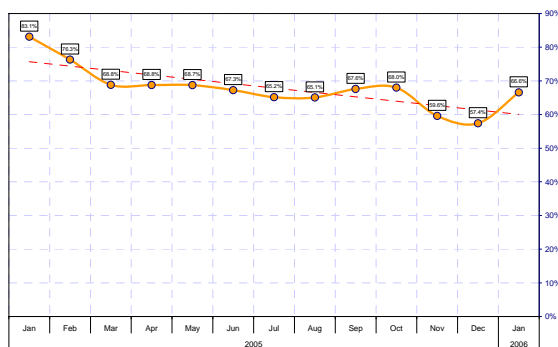
Introduction

Welcome to the January edition of the MessageLabs Intelligence monthly report. This report provides the latest threat trends for January 2006 to keep you informed and forearmed 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.

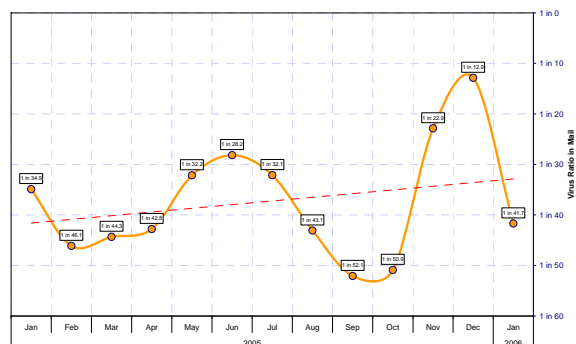
Spam Protection: In January, the global ratio of spam in email traffic from new and unknown bad sources, for which the recipient addresses were deemed valid, was 66.6% (1 in 1.5), an increase of 9.2% on the previous month.



Global Patterns of Spam Interceptions

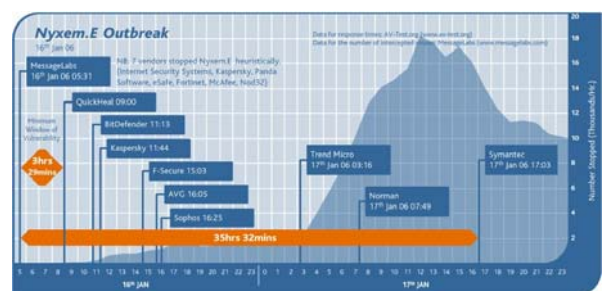
Anti-Virus and Trojan Protection: The global ratio of email-borne viruses in email traffic from new and previously unknown bad sources and destined for valid recipients, was 1 in 41.7 (2.4%), a decrease of 5.4% since the previous month.

MessageLabs, stopped over 4 million copies of Nyxem.E (also referred as MyWife.D, BlackWorm and Kama Sutra) during the first week of its propagation. The worm was scheduled to begin destroying files on infected machines and networks on Friday, February 3rd.



Global Patterns of Virus Interceptions

During the final week before the date the virus was due to activate, MessageLabs tracked over 11,000 computers being disinfected each day, leaving around 20,000 IP addresses that were still active on the trigger date, many of which were believed to reside in India. Furthermore, each IP address could still relate either to a single computer or to an organisation with several hundred computers, so it would be difficult to determine the full scale of the damage caused.



It seems as though this virus was created purely for malicious intent, unlike the majority of viruses we see today that create backdoors as a means to send spam or steal data.

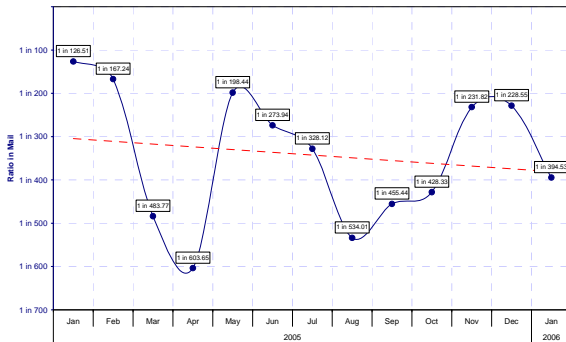
From the chart above, it can be seen that although there was a two-week window before the virus was due to activate, independent research shows that many traditional anti-virus updates were not available until up to 30 hours after the start of this outbreak. It is interesting to note also that seven vendors were able to detect this strain heuristically, i.e. a judgement based on the properties of the code rather than



through a signature. Most vendors will follow-up heuristic detection by also releasing a signature, since they offer no guarantees around their heuristic performance. A fine balance exists in having more aggressive heuristics that tend to result in higher rates of false positives - false positives occur when something is incorrectly identified as malicious – and this balance must also be struck with the limitation imposed by the resources available to these products without compromising the performance of the users.

By comparison, MessageLabs Skeptic™ technology was able to detect and stop the virus from its first instance, without the need for a signature and by utilising fairly aggressive artificial intelligence techniques that do not result in a high degree of false positives.

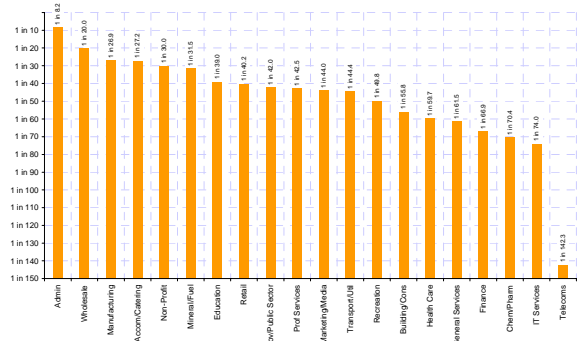
Phishing: January shows a decline in the proportion of phishing attacks in emails following the holiday season. However, the ratio of phishing as a proportion of malware has increased by 4.9% and accounts for 10.6% of malware intercepted by MessageLabs in January.



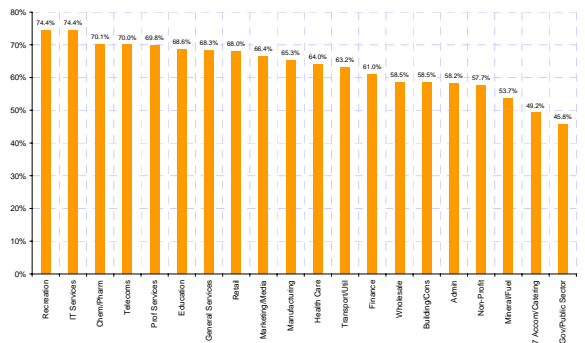
Global Patterns of Phishing Interceptions

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 January 2006:



Vertical Breakdown of Viruses Intercepted

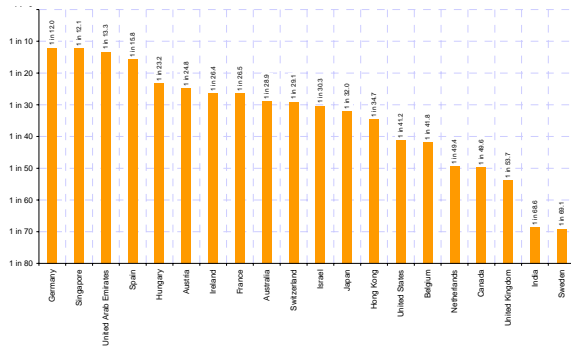


Vertical Breakdown of Spam Intercepted

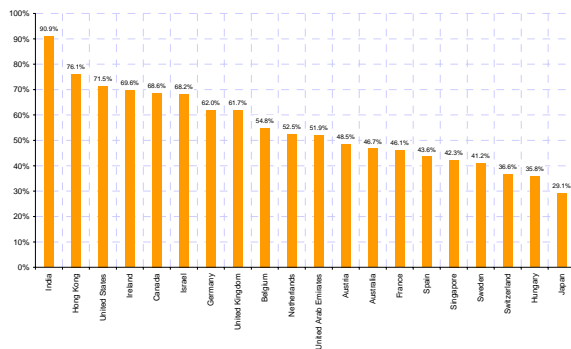


Geographical Breakdown

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 January 2006:



Geographical Breakdown of Viruses Intercepted



Geographical Breakdown of Spam Intercepted

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 organisation 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 January, on average, 6.8% 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 January, on average, 12.0% 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.

Region	Connection Management	
	SMTP Validation (botnet sources)	User Validation (directory attacks)
USA	7.2%	11.6%
UK	6.2%	13.2%
Europe	6.3%	14.1%
Asia Pacific	7.5%	3.0%
Worldwide	6.8%	12.0%

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.