

MessageLabs Intelligence: November 2005

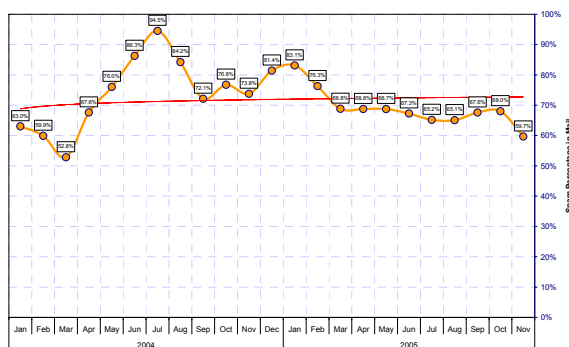
Introduction

Welcome to the November edition of the MessageLabs Intelligence monthly report. This report provides the latest email threat trends for November 2005 to help in the ongoing fight against unwanted email from spam, viruses and other unwelcome sources.

Global Trends & Content Analysis

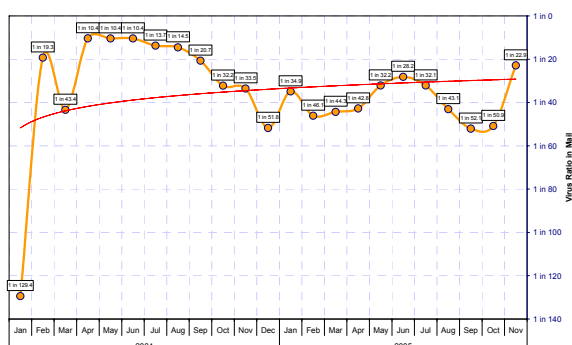
MessageLabs Anti-Spam and Anti-Virus Services focus on identifying and averting unwanted emails originating from unknown bad sources (such as fresh proxies) and which are addressed to valid email recipients.

Spam Protection: In November, the global ratio of spam in email traffic from new and unknown bad sources, for which the recipient addresses were deemed valid, was 59.6% (1 in 1.68), a drop of 8.4% from the previous month, largely due to the Sober.Y outbreak, being intercepted by the MessageLabs anti-virus service, but diluting the overall mail volumes.



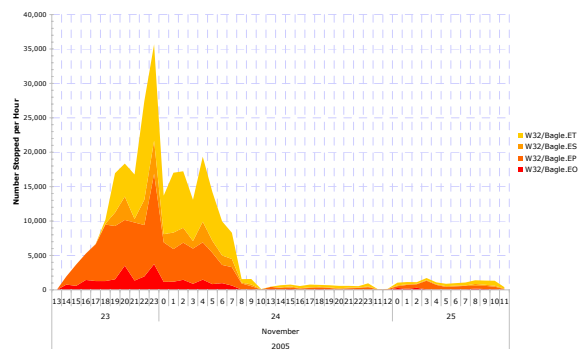
Global Patterns of Spam Interceptions

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 22.9 (4.4%), an increase of 2.4% since the previous month. This sharp rise was owing to the outbreak of Sober.Y, of which MessageLabs intercepted more than 46.1-million copies in the time between the first copies broke on the 21st November and the end of the month.



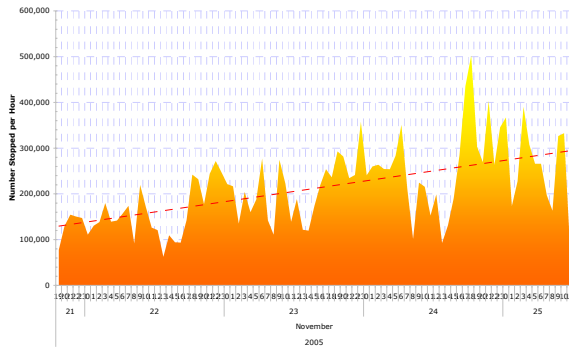
Global Patterns of Virus Interceptions

Although the largest outbreak of the year so far, Sober wasn't the only new virus to appear during November, as new strains of MyTob and Bagle were also in circulation.



Bagle.EO, EP, ES, ET: Mails Intercepted per Hour

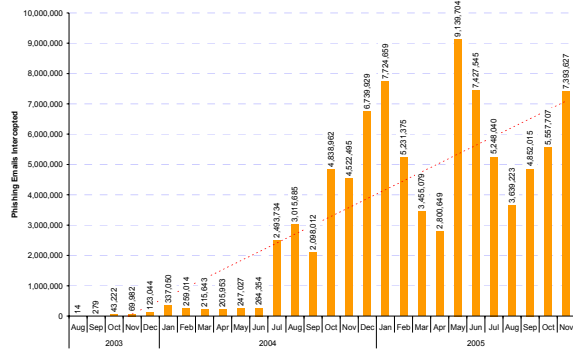
November is often a busy month as the botnet controllers begin to reinforce their botnets in the run-up to the Christmas holiday period, when these botnets are rented out to the spam sweatshops and spyware merchants in order for them to pump out their 'festive' messages.



Sober.Y: Mails Intercepted per Hour

Although many anti-virus vendors already had 'generic' detection available for Sober by 16th November, it highlights the fact that if your computer becomes ensnared in such a botnet, then your anti-virus defences are effectively down. Millions of computers already infected had their anti-virus software effectively disarmed by the trojan already installed on their computers.

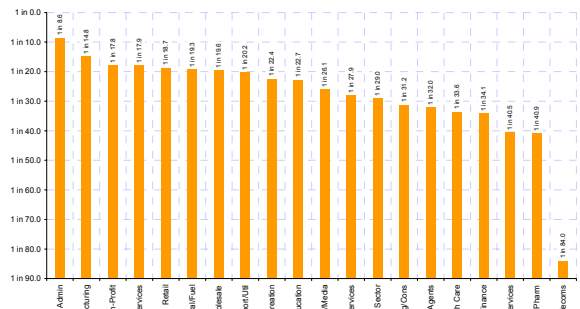
Phishing: November shows a further increase in phishing attacks, again perhaps not surprising in the run-up to the Christmas holiday season.



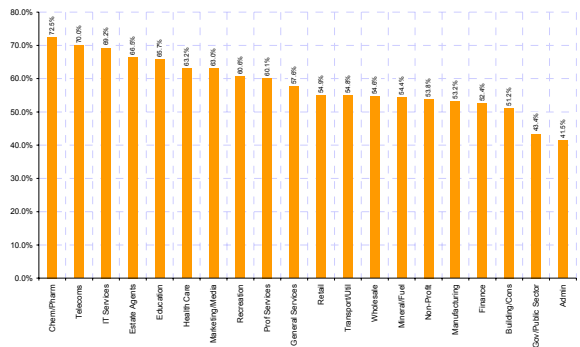
Global Patterns of Phishing Interceptions

Vertical Industry Breakdown

By analysing 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 November 2005:



Vertical Breakdown of Viruses Intercepted

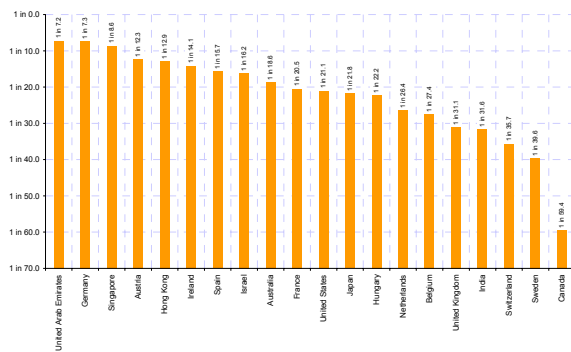


Vertical Breakdown of Spam Intercepted

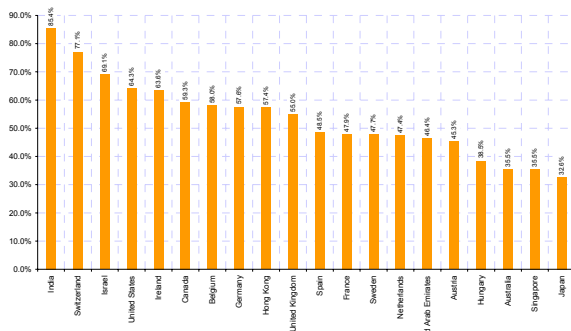


Geographical Breakdown

By analysing 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 November 2005:



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 November, on average, 9.7% of inbound messages were intercepted from botnets and other known malicious sources and rejected as a consequence, an increase of 5% on the previous month.

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 November, on average, 15.7% 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	7.8%	25.9%
UK	9.6%	3.0%
Europe	10.3%	12.5%
Asia Pacific	18.5%	1.9%
Worldwide	9.7%	15.7%

Effects of Connection Management Techniques



MessageLabs is the world's leading provider of email security and management services with more than 12,000 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.