



MessageLabs Intelligence: April 2007 “Email’s Double Whammy: Spam Messages Now with Viruses”

Introduction

Welcome to the April 2007 edition of the MessageLabs Intelligence monthly report. This report provides the latest threat trends and statistics to keep you informed regarding the ongoing fight against viruses, spam and other unwelcome content.

Top line results of this report include:

Spam – 76.1% in April (an increase of 0.9% since March)

Viruses – One in 145.5 emails in April contained malware (a decrease of 0.003% since March)

Phishing – One in 416.1 emails comprised a phishing attack (a fall of 0.08% since March)

In what is set to become one of the defining moments of this year, the gap has finally closed on the mutually beneficial convergence between viruses and spam. Each is already dependent upon the other to endure. And now, one criminal group has found a way to combine these two functions, the spam message and the virus code, into a single email, killing two birds with one stone. Since April 14, MessageLabs spam honeypots have already caught 3.5 thousand occurrences of these emails.

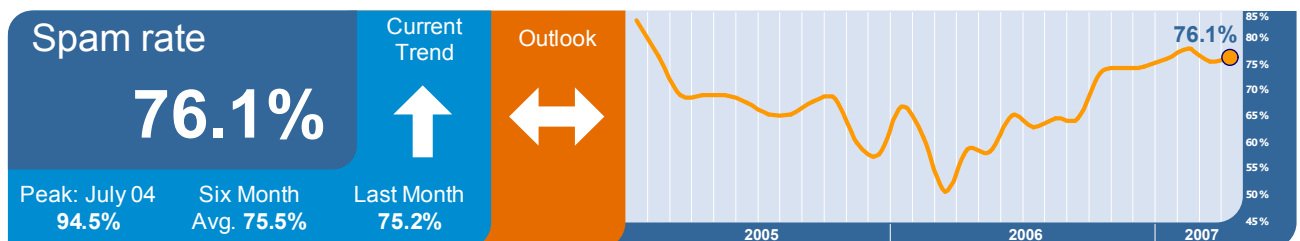
In April, new information emerged as to how this convergence works. The latest strains of Zhelatin (aka Storm Worm) are being spammed out in stock pump-and-dump emails which contain links to the new malware being hosted on websites under the control of the attackers. Purporting to be a screensaver, the malware contained in the link actually drops the Zhelatin MeSpam engine onto the compromised computer.

Until now, new versions of Zhelatin have been distributed via botnets to create larger botnets for the purposes of spamming. As the months progress this is now an area to which MessageLabs will pay close attention.

Global Trends & Content Analysis

MessageLabs Anti-Spam and Anti-Virus Services focus on identifying and averting unwanted communications originating from new and unknown bad sources that are addressed to valid email recipients.

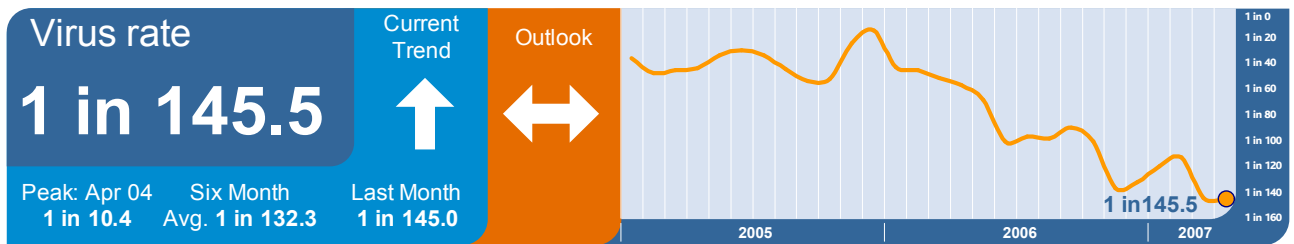
Skeptic™ Anti-Spam Protection: In April 2007, the global ratio of spam in email traffic from new and unknown bad sources, for which the recipient addresses were deemed valid, was 76.1% (1 in 1.31 emails), an increase of 0.9% on the previous month.



The figure of 76.1% is actually lower than the “true” spam figure since MessageLabs Traffic Management enables control of the amount of bandwidth given to absolutely known bad-sources of spam and then throttles those connections, slowing them down to a crawl. To the spammer, it appears they are talking to a very slow modem.

In turn, this makes it incredibly painful for spammers attempting to send spam to MessageLabs clients as Traffic Management effectively pushes the spam back to the spammers’ networks and slows down the ability to send lots of spam. Consequently, many such connections eventually “time-out” or move on to softer targets. If we look at the amount of spam hitting MessageLabs honey-pots, which are unprotected by comparison, this figure would be much closer to 83.6%. For further information, please refer to the section on Traffic Management later in this report.

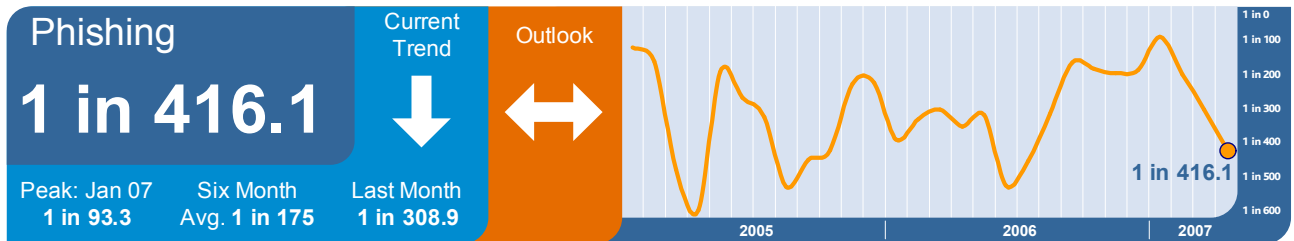
Skeptic™ Anti-Virus and Trojan Protection: The global ratio of email-borne viruses in email traffic from new and previously unknown bad sources destined for valid recipients, was 1 in 145.5 emails (0.69%) in April, a decrease of 0.003% since last month.



This month MessageLabs conducted analysis on the highly specialized targeted attacks intercepted during the previous month. Overall MessageLabs stopped 716 emails in 249 targeted attacks in the month of March. Two-hundred sixty three different domains were targeted, belonging to 216 different customers. It was found that 84% of the attacks used Microsoft Office exploits: 45% of the attacks exploited vulnerabilities in Microsoft PowerPoint, and 35% exploited Microsoft Word; indicating that PowerPoint has overtaken Word as the most common exploit vector since this time last year. The majority of attacks still comprise one email to one individual, but the number of attacks has risen since last year when it was just 1 or 2 per day.

Utilizing several exploits in a single malicious file, a typical attack will download a further component from a website under the control of the attackers that will give them remote access to the compromised computer, including access to confidential and potentially sensitive intellectual property.

Phishing: April showed a decrease of 0.08% in the proportion of phishing attacks compared with the previous month. One in 416.1 (0.24%) emails comprised some form of phishing attack.



However, when judged as a proportion of all email-borne threats such as viruses and trojans, the quantity of phishing emails has fallen to levels last seen in August 2006. 35% of all malicious emails intercepted by MessageLabs in April were phishing attacks, a decrease of 12% on the previous month. This is due to a drop in the overall level of phishing activity compared with March, while virus levels remained fairly static.

Skeptic™ Web Security Services Version 2.0: MessageLabs Web Security Services version 2.0, built on MessageLabs proprietary technology using Skeptic, enables MessageLabs to take the very latest threat and reputation information from other protocols, such as email, and apply that knowledge to web traffic.

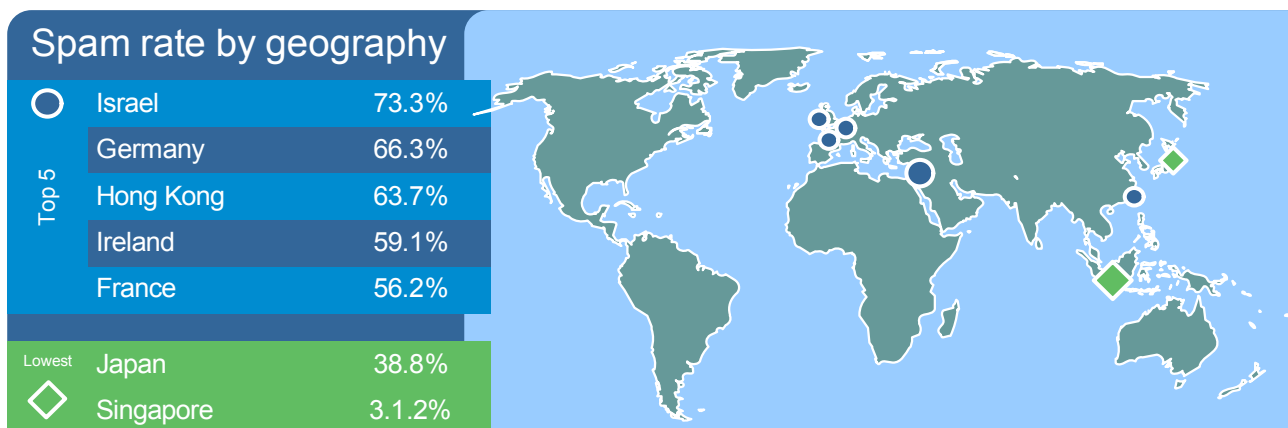
Web Security Services (Version 2.0) Activity:					
Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisements & Popups	55.76%	Trojan-Downloader.Win32.IstBar.pk	74.21%	Adware-GAIN	63.64%
Spyware	6.99%	Trojan-Downloader.Win32.Agent.yg	3.52%	Adware-SaveNow	31.36%
Unclassified	6.45%	VBS/Psyme	3.48%	Adware-ISTbar.b	4.71%
Adult/Sexually Explicit	5.13%	JS/Downloader-AUD	1.64%	AdwareDropper-l.gen	0.04%
Streaming Media	4.12%	Generic Downloader.o	1.37%	Adware-TCent	0.04%
Chat	3.32%	Exploit-ANIfile.c	1.30%	Adware-DFC	0.03%
Shopping	3.24%	Suspicious IFrame -c	1.02%	Adware-NaviPromo	0.02%
Personals & Dating	2.53%	JS/Wonka	0.98%	Adware-DropSpam	0.02%
Gambling	2.33%	Trojan-Downloader.VBS.Agent.u	0.84%	Adware-HotBar	0.02%
Downloads	1.38%	JS/Downloader-BAU	0.61%	Adware-ZangoSA	0.02%

It can be seen from the chart above that Advertisements & Popups (55.76%) is the most common trigger for policy-based filtering applied by MessageLabs for its business clients. This is an increase of 0.4% on the previous month. Further analysis shows that 6.4% of the malware intercepted was new in April.

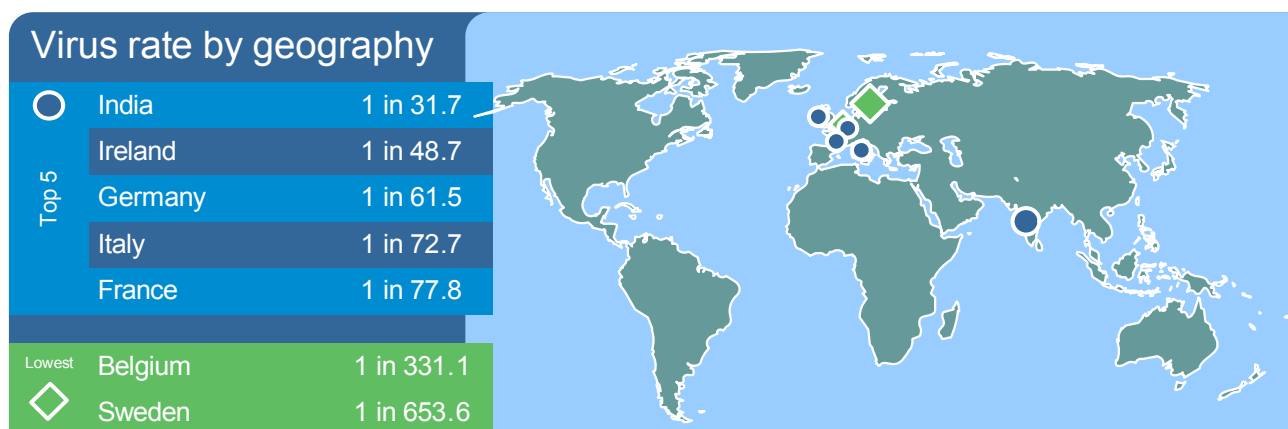
The “Unclassified” category identifies new and previously uncategorized sites that may potentially need to be prohibited. The Unclassified category affords more confidence when defining new rules. This means that newly detected malicious sites may be handled more appropriately until categorized, thereby safeguarding against domain kiting sites which may appear and disappear within a 24 to 48 hour timeframe. Such sites may be used for disreputable purposes, such as hosting phishing and spam sites, disseminating information-stealing trojans and other fraudulent activities. 94.5% of web Viruses and 81.9% of Spyware intercepted were classified in this category, suggesting that the majority of these interceptions were hosted on web sites that were previously unknown and uncategorized.

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 April 2007.



Spam levels in Israel fell by only 0.3% this month, as the region continues to be heavily targeted. Levels in Germany rose by 10.3% in April which took it into second place, while spam in Hong Kong fell by 1.5%. Spam destined for Ireland increased by 2%, and France by 1.2%. A decrease of 7% was observed in Japan; however the largest fall occurred in New Zealand with a drop of 10%, taking New Zealand to the bottom of the table.



The largest increase in virus activity was noted in India, where levels rose by 2.2%, making India the most targeted region this month. Close behind is Ireland which received the second highest increase of 1%. Italy also bore an increase in April of 0.8%. Decreases were noted in France and Germany by 0.2% and 0.6% respectively. At the bottom of the rankings, New Zealand saw a fall of 0.01%, and virus activity in Sweden, the least attacked country, fell by 0.76%.

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 April 2007.

Spam rate by vertical			Virus rate by vertical		
Top 5	Manufacturing	62.1%	Top 5	Education	1 in 60.4
	Education	61.3%		Business Support Services	1 in 77.3
	Wholesale	57.6%		Retail	1 in 82.5
	Business Support Services	57.5%		Chem/Pharm	1 in 112.3
	IT Services	56.1%		Wholesale	1 in 114.4
Lowest	Gov/Public Sector	40.1%	Lowest	Transport/Util	1 in 247.1
	Finance	35.1%		Telecoms	1 in 526.9

Spam levels for Manufacturing fell by 2.6% this month, and a fall of 0.3% was observed in the Education sector. An increase in spam activity was noted for the Wholesale sector with a rise of 0.9%; however, the greatest increase occurred in the Business Support Services sector where levels rose by 16.3%. Spam levels in the IT Services sector fell by 3.5% between March and April. Spam levels across Government and Public Sector bodies fell by 3.3% this month, and a fall of 1.8% was noted across the Finance sector also, making the vertical the least targeted sector for spam in April.

The largest rise in virus traffic occurred in the Education sector, the most targeted sector in April, where levels rose by 0.5% since March. Virus activity for the Business Support Services vertical fell by 0.1%, while an increase of 0.3% was noted across the Retail sector. Virus activity targeting the Chemical & Pharmaceutical sector also rose by 0.03% this month, while attacks against the Wholesale sector fell by 0.1%. The Telecommunications sector continues to be the least targeted vertical in April, and virus levels fell by 0.02% this month. Virus activity in the Transport & Utilities sector also fell by 0.1%.

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 using features embedded in the TCP protocol. Incoming volumes of known spam are significantly slowed, while legitimate email is expedited.

In April, MessageLabs processed more than 2.1 billion SMTP connections per day, of which 88.1% were throttled back as a result of traffic management protocol controls for traffic that was unequivocally malicious or unwanted. The remainder of these connections is subsequently processed by MessageLabs Connection Management controls and Skeptic™.

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. It 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 April, an average of 43.2% of inbound messages was 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 April, an average of 5.6% of recipient addresses was identified as invalid. These were attempted directory attacks on domains that were prevented as a result.

Summary

The table below details the current impact of traffic and 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 April would otherwise account for around 83.6% of global email traffic, an increase of 0.5% on the previous month.

Region	Traffic Management (protocol control)	SMTP Validation (behaviour analysis)	User Validation (directory attacks)
USA	91.0%	47.9%	4.8%
UK	82.1%	38.9%	4.8%
Europe	76.6%	35.7%	8.7%
Asia Pacific	65.7%	40.8%	1.1%
Worldwide	88.1%	43.2%	5.6%

Effects of Traffic Management Techniques

MessageLabs is a leading provider of integrated messaging and web security services, with over 15,000 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 (April 2007)

	April	March	Change
Australia	40.0%	41.3%	-1.3%
Austria	51.4%	50.5%	0.9%
Belgium	48.5%	46.9%	1.6%
Canada	53.6%	55.9%	-2.3%
China	41.5%	50.0%	-8.5%
France	56.2%	55.0%	1.2%
Germany	66.3%	56.0%	10.3%
Hong Kong	63.7%	65.2%	-1.5%
India	44.4%	45.2%	-0.8%
Ireland	59.1%	57.1%	2.0%
Israel	73.3%	73.6%	-0.3%
Italy	48.0%	54.4%	-6.4%
Japan	38.8%	31.8%	7.0%
Netherlands	39.8%	36.0%	3.8%
Singapore	31.2%	50.8%	-19.6%
Spain	51.0%	33.4%	17.6%
Sweden	48.6%	40.4%	8.2%
Switzerland	46.6%	49.6%	-3.0%
United Arab Emirates	45.3%	47.5%	-2.2%
United Kingdom	47.5%	46.4%	1.1%
United States	55.9%	60.2%	-4.3%

Appendix II: Virus Rate by Geography (April 2007)

	April	March	Change
Australia	0.41%	0.41%	0.00%
Austria	0.99%	1.06%	-0.07%
Belgium	0.30%	0.44%	-0.14%
Canada	0.57%	0.63%	-0.06%
China	1.17%	0.96%	0.21%
France	1.29%	1.51%	-0.22%
Germany	1.63%	2.23%	-0.60%
Hong Kong	1.03%	1.00%	0.03%
India	3.16%	2.88%	0.28%
Ireland	2.05%	1.10%	0.95%
Israel	0.72%	0.56%	0.16%
Italy	1.38%	0.82%	0.56%
Japan	0.59%	0.51%	0.08%
Netherlands	0.34%	0.43%	-0.09%
Singapore	1.20%	1.13%	0.07%
Spain	1.02%	0.91%	0.11%
Sweden	0.15%	0.44%	-0.29%
Switzerland	1.20%	1.21%	-0.01%
United Arab Emirates	1.12%	0.78%	0.34%
United Kingdom	0.67%	0.61%	0.06%
United States	0.70%	0.72%	-0.02%

Appendix III: Spam Rate by Vertical (April 2007)

	April	March	Change
Accom/Catering	45.1%	44.1%	1.0%
Agriculture	55.0%	54.5%	0.5%
Building/Cons	42.7%	41.2%	1.5%
Business Support Services	57.5%	45.2%	12.3%
Chem/Pharm	52.1%	55.1%	-3.0%
Education	61.3%	61.6%	-0.3%
Estate Agents	41.0%	35.0%	6.0%
Finance	35.1%	36.9%	-1.8%
General Services	44.0%	31.7%	12.3%
Gov/Public Sector	40.1%	43.4%	-3.3%
Health Care	52.6%	53.2%	-0.6%
IT Services	56.1%	59.6%	-3.5%
Manufacturing	62.1%	64.7%	-2.6%
Marketing/Media	55.5%	59.1%	-3.6%
Mineral /Fuel	48.9%	50.6%	-1.7%
Non-Profit	45.0%	43.3%	1.7%
Prof Services	49.8%	51.5%	-1.7%
Recreation	44.4%	46.1%	-1.7%
Retail	50.6%	52.2%	-1.6%
Telecoms	47.5%	54.6%	-7.1%
Transport /Util	52.6%	53.9%	-1.3%
Wholesale	57.6%	56.7%	0.9%

Appendix IV: Virus Rate by Vertical (April 2007)

	April	March	Change
Accom/Catering	0.44%	0.90%	-0.46%
Agriculture	0.41%	0.38%	0.03%
Building/Cons	0.46%	0.44%	0.02%
Business Support Services	1.29%	1.40%	-0.11%
Chem/Pharm	0.89%	0.86%	0.03%
Education	1.66%	1.23%	0.43%
Estate Agents	0.52%	0.52%	0.00%
Finance	0.54%	0.53%	0.01%
General Services	0.56%	0.46%	0.10%
Gov/Public Sector	0.72%	0.72%	0.00%
Health Care	0.64%	0.72%	-0.08%
IT Services	0.79%	0.79%	0.00%
Manufacturing	0.79%	0.83%	-0.04%
Marketing/Media	0.80%	0.83%	-0.03%
Mineral /Fuel	0.54%	0.65%	-0.11%
Non-Profit	0.58%	0.67%	-0.09%
Prof Services	0.75%	0.77%	-0.02%
Recreation	0.59%	0.63%	-0.04%
Retail	1.21%	0.90%	0.31%
Telecoms	0.19%	0.21%	-0.02%
Transport /Util	0.40%	0.53%	-0.13%
Wholesale	0.87%	0.94%	-0.07%