MessageLabs®

Be certain

MessageLabs Intelligence: Q1/March 2008
“One Fifth of All Spam Springs from Storm Botnet”

Welcome to the March edition of the MessageLabs Intelligence monthly report. This report provides the latest threat trends for March 2008 to keep you informed regarding the ongoing fight against viruses, spam and other unwelcome content.

Report Highlights

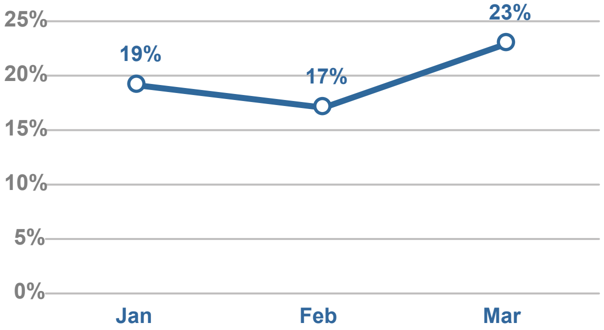
- Spam – 73.8% in March (an increase of 1.1% since February)
- Viruses – One in 169.2 emails in March contained malware (a decrease of 0.36% since February)
- Phishing – One in 228.7 emails comprised a phishing attack (a decrease of 0.57% since February)
- 20% of all spam in Q1 is Storm-generated
- Spoofing in the Web 2.0 age
- Latest form of image spam sticks out

Report Analysis

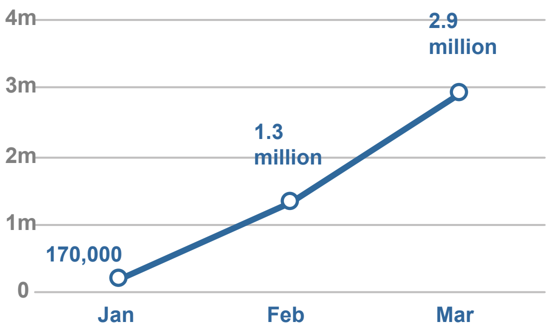
Storm responsible for around 20% of all spam in Q1 2008
Since its birth in January 2007, the size and scope of the Storm botnet has remained somewhat of a mystery to some within the security industry. Some reports point to the botnet shrinking or being overtaken by newer botnets whilst others claim that Storm simply undergoes quiet periods before ramping up to compete with emerging botnets on the scene.

In reality, Storm has been partitioned into smaller more discreet segments, each rented to different spammers, but still a part of the same overall Storm botnet, according to MessageLabs research. In addition to spamming, some parts of the botnet are also used to spread malware and launch phishing attacks. MessageLabs tracked the total volume of Storm-generated spam during Q1 2008 and the number of emails received that contain links to Storm malware, intended to grow the botnet.

Use of Storm: % of spam originating from Storm



Growing Storm: Number of emails received containing links to Storm malware



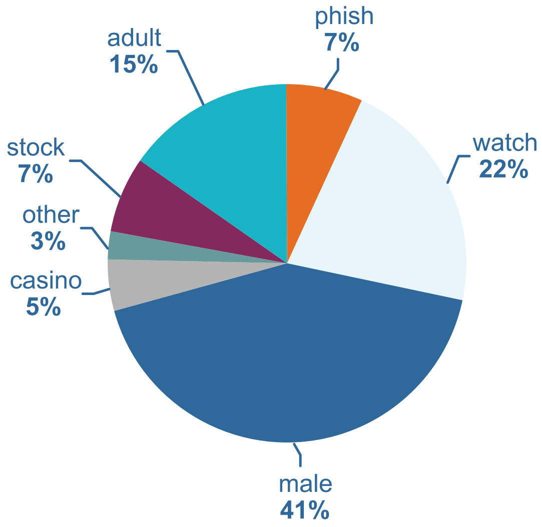
During the first quarter of 2008, the volume of spam emanating from the Storm botnet accounts for approximately 20 percent of all spam – one in every five spam messages sent. The figure fluctuates slightly during the three months from a ‘low’ of 17% in February and the highest levels experienced during March, when 23% of all spam intercepted originated from the Storm botnet.

The proportion of Storm-related malware has also grown significantly over the first quarter of the year. In January, MessageLabs intercepted over 17,000 Storm-generated emails containing links to the Storm malware. The majority of subject lines related to New Year’s resolutions, as reported in the January MessageLabs Intelligence report. The volume significantly increased in February, when 1.3 million malware links were intercepted by MessageLabs with subject lines about St. Valentine’s Day including spam touting VPXL, a drug promising male sex organ enlargement.

Most of the Storm-related malware intercepted in March purported to be fake e-Greeting cards and spoofed postcard sites. By the end of the month, 2.9 million emails containing malicious Storm links had been intercepted. Although in March the proportion of email-borne malware identified containing a link to a Web site hosting malicious content decreased by 17.6% to 43.5%, of those, 96% were Storm-related.

For Q1, the breakdown of categories for spam emanating from the Storm botnet is as follows:

Spam from Storm Q1 2008

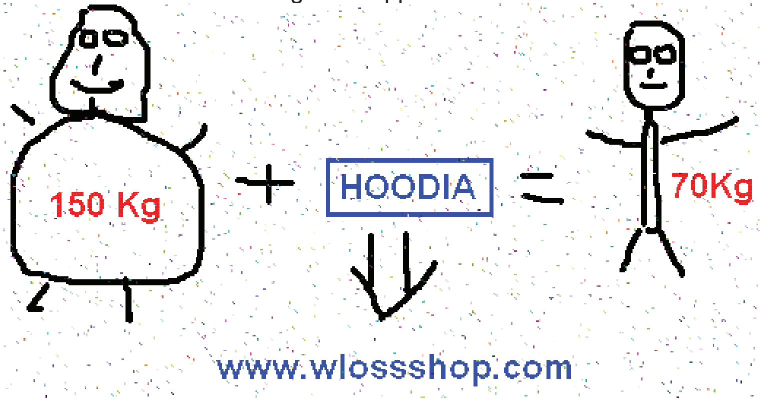


Spoofing in the age of Web 2.0
Fake versions of high profile personalities and celebrities, such as the Prince of Morocco, appearing on Facebook have made headline news recently (http://news.bbc.co.uk/1/hi/world/africa/7304361.stm). With social networking becoming so widespread and user-friendly interfaces, it raises the question as to whether spoofing could also happen in the corporate environment. MessageLabs Intelligence reveals that when it comes to identity fraud, spoofing is a major risk. Recent intelligence reveals this is indeed happening. Whilst your profile may not attract as much media attention as the Prince of Morocco, it may certainly be more highly prized when it comes to identity fraud.

Whilst corporate users continue to adopt Facebook and other social networking sites in droves, organizations are now becoming wise to negative business implications of these tools. When analyzing MessageLabs customers with Web Security Services, 11% have already become wise to the risk associated with social networking and have set up rules to block access specifically to Facebook. When comparing this figure to the 3% of clients who have pro-actively set up rules to allow access, it questions if the Facebook bubble in the work place is bursting?

Stick-man spam: The latest form of image spam?

A new, albeit not very effective type of image-spam, began on the evening of 6 March. MessageLabs believes this “stick-man” spam may be the first of its kind using very amateur-looking artwork to advertise weight loss drugs such as Hoodia. The image is embedded in the message and appears as below in the email:



The spam was being distributed in small batches from botnet infected computers, but in relatively low numbers as it accounted for less than 1% of spam overall. Although the spam-run appeared the same, the images were randomized by including background-noise pixels and changing subject lines in order to evade signature detection. For example:

Subject: `150Kg + H = 75Kg`
Subject: `150Kg + Hoodia = 75Kg`
Subject: `Become thin`
Subject: `Best Weight Loss`
Subject: `Lose 20 pounds`
Subject: `Lose 20 pounds in 3 weeks`
Subject: `Problems with weight?`
Subject: `Pure Hoodia Weight Loss`
Subject: `Thin`

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 2008, the global ratio of spam in email traffic from new and previously unknown bad sources, was 73.8% (1 in 1.36 emails), an increase of 1.1% on the previous month. An additional 5.8% of spam was removed using MessageLabs traffic management controls, based on the profile of known bad sources. Without these controls the overall proportion of spam would be around 79.6%, a decrease of 3.1% since February; indicating a slight fall in spam from known bad sources.

Spam rate

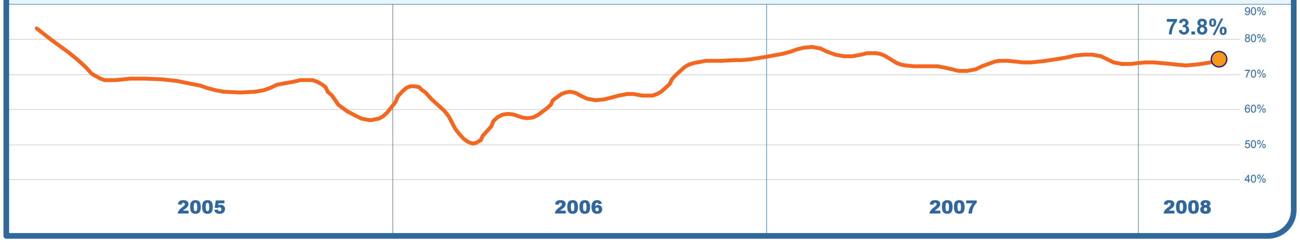
73.8%

Last Month:	72.7%
Six Month Average:	73.9%

Top 5 Geographies	
86.6%	Switzerland
85.0%	Hong Kong
80.9%	Israel
78.5%	Austria
76.8%	France

Top 5 Verticals	
82.1%	Manufacturing
80.4%	Education
79.9%	IT Services
79.6%	Non-Profit
79.2%	Agriculture

By horizontal	
74.3%	1-250
71.9%	251-500
73.7%	501-1000
75.4%	1001-1500
76.4%	1501-2500
69.8%	2501+



In March, Switzerland replaced Hong Kong as the most spammed country with levels reaching 86.6% of all email. Other than Singapore, Hong Kong, China, Canada and Australia, all countries received an increase in spam, with levels in Spain increased the most with a rise of 6.17%.

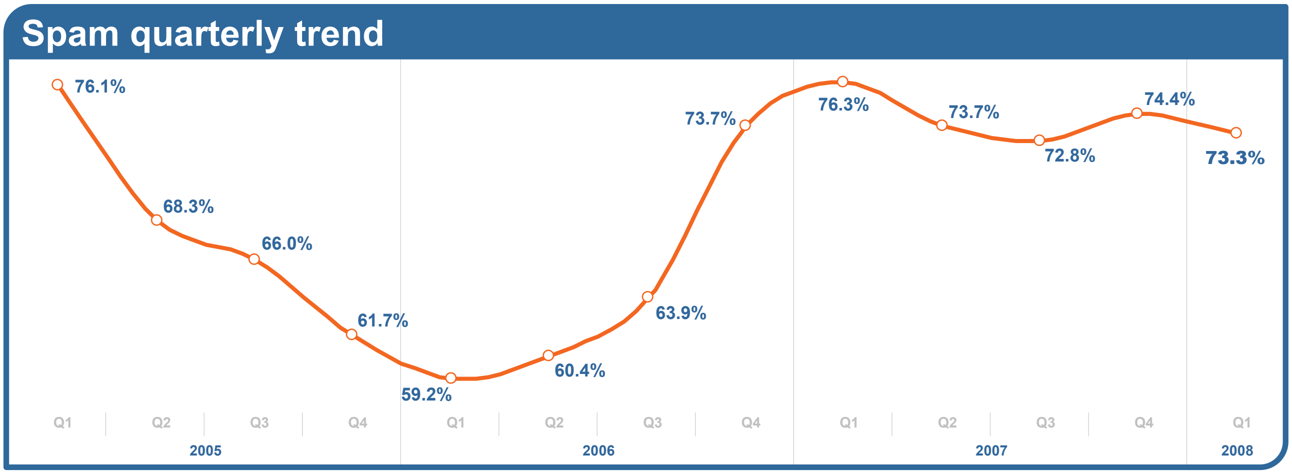
Spam levels in the US reached 70.7% in March, 69.1% in Canada and 61.1% in the UK. Germany's spam rate reached 70.1% and 68.6% in the Netherlands. Spam levels in Australia were 61.3%, 66.8% in New Zealand, 68.8% in China and 65.5% in Japan.

Spam levels fluctuated across many industry sectors in March, with Manufacturing and Education being the top two verticals for spam activities. The greatest rise was noted in the IT Services sector, where spam levels rose by 4.6% to 79.9%.

Chemical & Pharmaceutical sector spam levels reached 69.5%, 78.0% for Retail, 70.6% for Public Sector and 68.1% for Finance.

Enterprises which employed between 1501 – 2500 staff were targeted with more spam than its smaller counterparts, receiving more than the average spam levels, with a spam rate of 76.4%.

Quarterly Review: From the chart below it can be seen that spam levels for Q1 2008 are 1.1% lower than for Q4 2007, and 3% lower than for the same period in 2007, but 14.1% higher than in 2006.


Spam quarterly trend

Skeptic™ Anti-Virus and Trojan Protection: The global ratio of email-borne viruses in email traffic from new and previously unknown bad sources, was 1 in 169.2 emails (0.59%) in March, a decrease of 0.36% since the previous month.

Virus rate

1 in 169.2

Last Month:	**1 in 105.5**
Six Month Average:	**1 in 137.0**

Top 5 Geographies

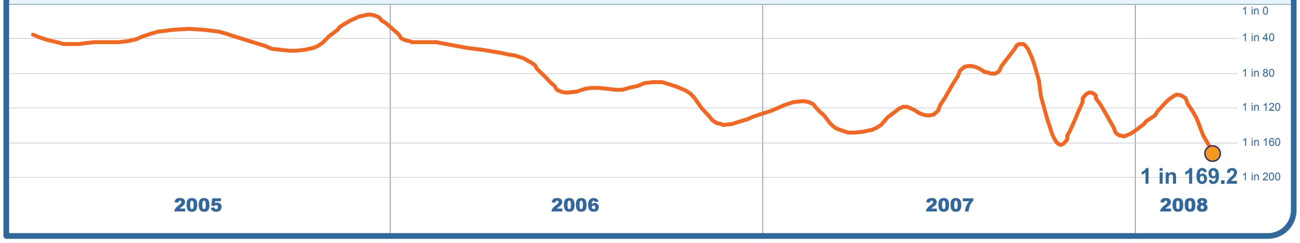
1 in 68.7	Switzerland
1 in 87.3	France
1 in 90.2	India
1 in 94.9	Austria
1 in 117.0	Israel

Top 5 Verticals

1 in 67.8	Accom/Catering
1 in 92.8	Education
1 in 114.3	Chem/Pharm
1 in 129.2	Wholesale
1 in 136.6	Mineral/Fuel

By horizontal

1 in 226.5	1-250
1 in 220.1	251-500
1 in 172.9	501-1000
1 in 120.0	1001-1500
1 in 111.2	1501-2500
1 in 209.0	2501+



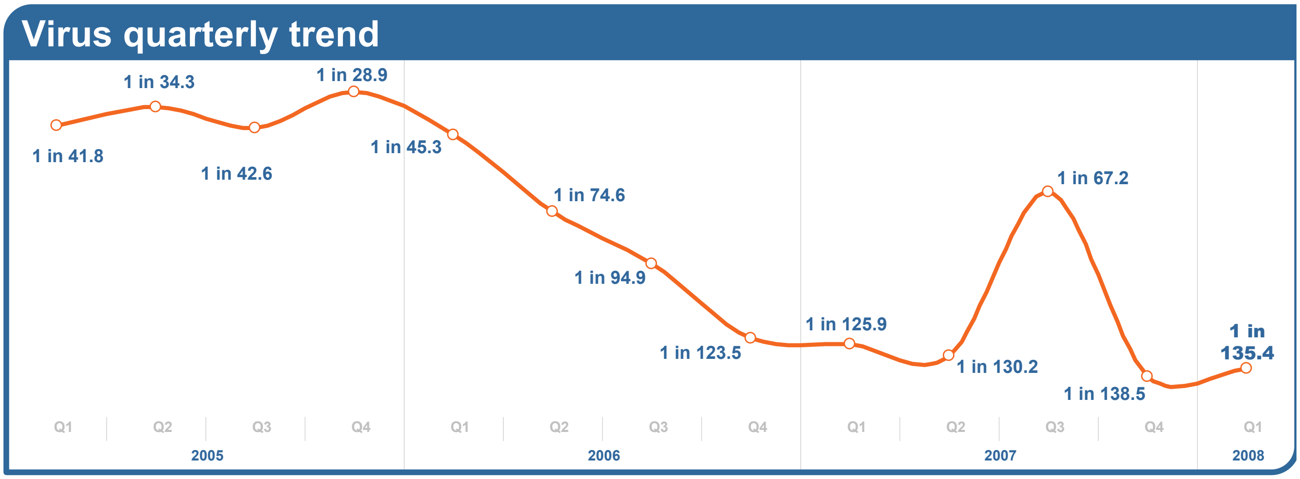
Virus activity fell across almost all regions in March, except in Austria, Italy and Sweden where levels increased by 0.33%, 0.06% and 0.02% respectively. The largest fall of 1.2% was observed in Israel, which falls from the top spot to fifth place in March. Despite a drop of 0.54%, Switzerland is the most targeted country for viruses with levels of 1 in every 68.7 emails.

Virus levels for the US were 1 in 245.1 and 1 in 180.3 for Canada. For the UK, levels reached 1 in 137.7 and 1 in 255.6 for Germany. In Australia, virus levels were 1 in 215.7 and 1 in 257.4 for Japan.

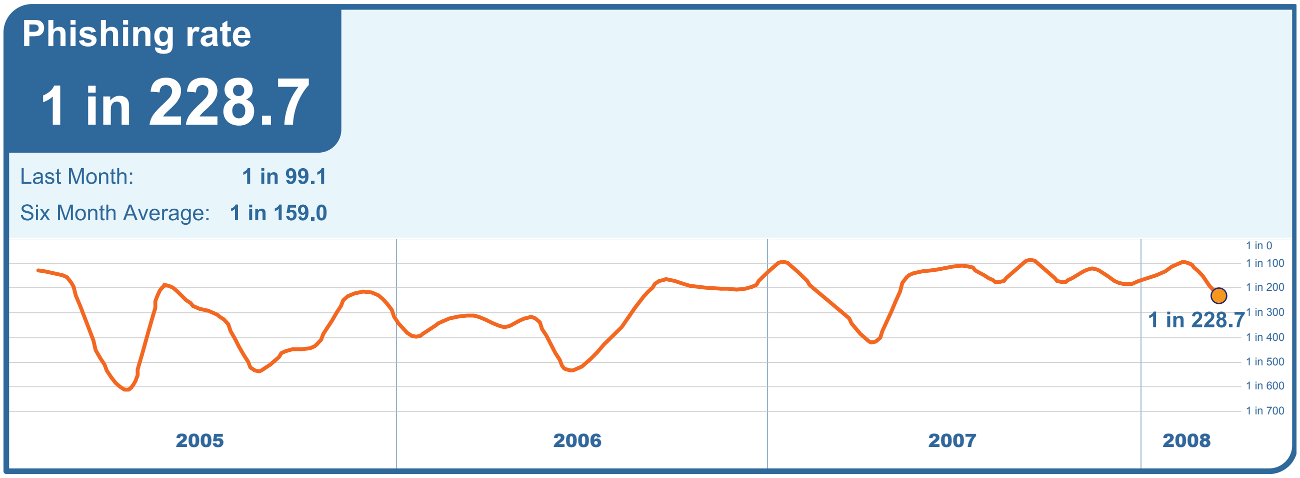
Similarly, virus levels across many industry sectors fell during March, with Education being the only exception where virus levels rose by 0.06. Accommodation/Catering received the most virus activity with 1 in 67.8 emails being infected. Virus levels for the IT Services sector were 1 in 232.2, 1 in 173.5 for Retail and 1 in 231.5 for Finance.

Larger sized businesses continue to be targeted with more viruses than Small to Medium sized businesses. For example, businesses sized 1-250 received 1 virus in every 226.5 emails, compared with businesses sized 1,501-2,500 which received 1 virus in 111.2 emails, and those with 2,500+ employees which received 1 per 209 emails.

Quarterly Review: From the chart below it can be seen that virus levels for Q1 2008 are 0.72% higher than for Q4 2007. Compared with Q1 2007, virus levels are 0.06% lower, and 1.47% lower than Q1 2006.


Virus quarterly trend

Phishing: March saw a decrease of 0.57% in the proportion of phishing attacks compared with the previous month. One in 228.7 (0.44%) emails comprised some form of phishing attack. When judged as a proportion of all email-borne threats such as viruses and Trojans, the number of phishing emails had fallen by 13.5% to 74.0% of all email-borne malware threats intercepted in March.


Phishing rate

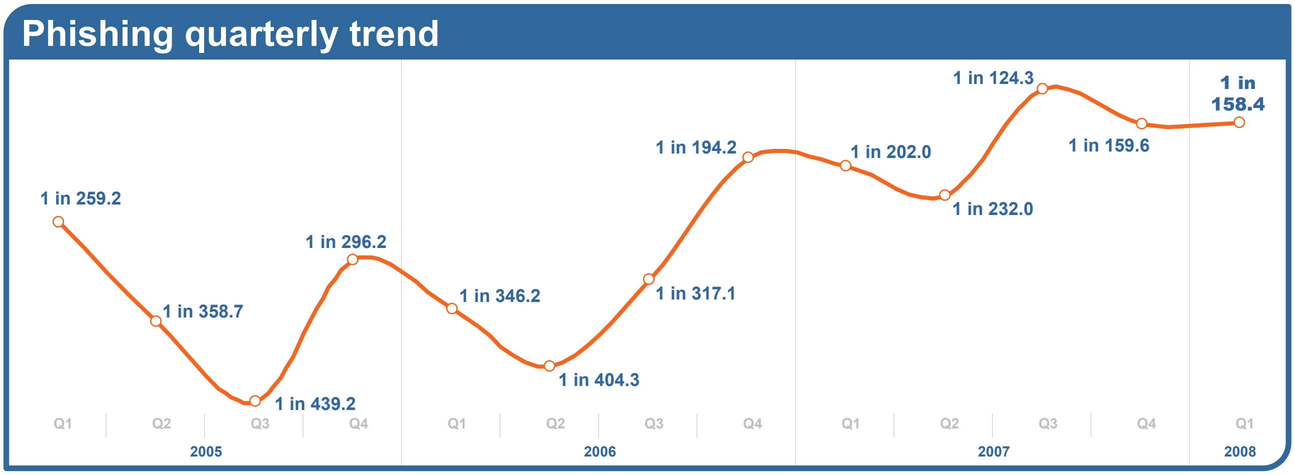
1 in 228.7

Last Month: 1 in 99.1

Six Month Average: 1 in 159.0

Quarterly Review: From the chart below it can be seen that phishing levels for Q1 2008 are almost unchanged from Q4 2007. Compared with Q1 2007, phishing levels are now 0.14% higher and 0.34% higher than Q1 2006.

Phishing quarterly trend



Skeptic™ Web Security Version 2.0: The most common trigger for policy-based filtering applied by MessageLabs for its business clients is the “Advertisements & Popups” category, up by 17.5% since February.

Analysis of web security activity shows that 9.2% of all web based malware intercepted was new in March. MessageLabs also identified an average of 595 new sites per day harboring malware and other potentially unwanted programs such as spyware and adware.

Web Security Services (Version 2.0) Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisements & Popups	51.7%	Suspicious IFrame.b	16.29%	PUP - AdTool.Win32.MyWebSe...	21.27%
Chat	24.7%	Suspicious IFrame.a	7.85%	PUP - Server-FTP.Win32.Tftpd.274	15.24%
Unclassified	6.7%	Trojan.JS.Redirector.e	6.34%	PUP - AdWare.Win32.Virtumonde.gen	7.47%
Streaming Media	5.4%	New JS-b	5.59%	PUP - RemoteAdmin.Win32.WinVNC.4	6.17%
Adult/Sexually Explicit	1.6%	Generic.dx	4.86%	PUP - AdWare.Win32.OneStep.c	5.18%
Personals & Dating	1.6%	HTML/IFrame	3.86%	PUP - AdWare.Win32.Shopper.r	3.66%
Photo Searches	1.0%	JS/Exploit-BO	3.71%	PUP - AdWare.Win32.SearchPage	2.29%
Gambling	1.0%	New Malware.f	3.35%	PUP - RemoteAdmin.Win32.WinVN...	2.21%
Web-based E-mail	1.0%	Phish-BankFraud.eml.b	2.51%	PUP - ZangoSA	2.06%
Proxies & Translators	0.8%	Exploit-IFrame	1.87%	PUP - AdWare.Win32.AdWeb.a	1.98%

The “Unclassified” category identifies new and previously uncategorized sites that may potentially need to be prohibited. This category accounted for 6.7% of the web traffic intercepted. The “Unclassified” category affords more confidence when defining new rules, which means that newly detected malicious sites may be handled more appropriately until categorized, thereby safeguarding against sites which 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, information-stealing Trojans and other fraudulent activities. 52.7% of all web-based viruses intercepted were classified in this category, as were 35.7% of all spyware, adware and other potentially unwanted programs.

The chart below also shows the breakdown of policies triggered by company size, highlighting the top-5 policies for each. Note that the “Unclassified” category (not listed below) was the fourth most triggered policy for companies 501-2,500 accounting for 1.5% of the activity.

Web Security Services (Version 2.0) Activity:

Policy-Based Filtering by Vertical

	1-500	501-2500	2501+
Advertisements & Popups	50.9%	32.5%	70.6%
Chat	16.8%	52.7%	16.6%
Streaming Media	11.5%	7.9%	1.9%
Adult/Sexually Explicit	0.6%	1.1%	3.7%
Personals & Dating	1.9%	0.6%	2.3%
Gambling	1.0%	0.8%	2.0%
Proxies & Translators	3.2%	0.1%	0.2%
Games	0.4%	0.1%	1.7%
Spyware	1.6%	0.9%	0.2%
Web-based E-mail	2.1%	0.2%	0.0%

Top 5

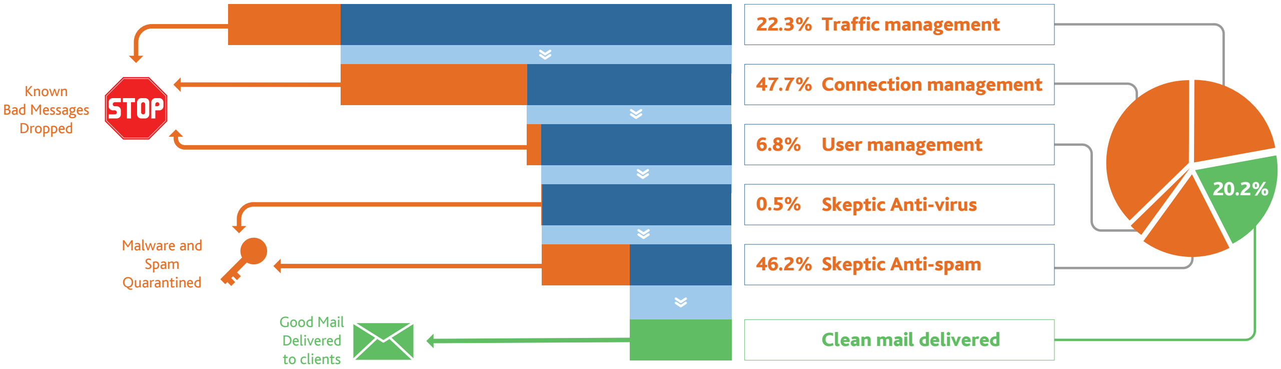
New Malware Sites per Day

New sites with **spyware**	101/day
New sites with **web viruses**	494/day
Total	**595/day**

Traffic Management

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.

In March, MessageLabs processed an average of 3.89 billion SMTP connections per day, of which 22.3% were throttled back as a result of traffic management controls for traffic that was unequivocally malicious or unwanted. The remainder of these connections was 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, using SMTP Validation techniques. It is able to identify 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, an average of 47.7% of inbound messages was intercepted from botnets and other known malicious sources and rejected as a consequence.

User Management

User Management uses Registered User Address Validation techniques to reduce the overall volume of emails for registered domains, by discarding connections for which the recipient addresses are identified as invalid or non-existent. In March, an average of 6.8% of inbound messages was identified as invalid; these were attempted directory attacks upon domains that were therefore prevented.

MessageLabs Intelligence
MessageLabs Intelligence is a respected source of data and analysis for email, web and IM security issues, trends and statistics. Securing more than 2.5 billion email connections and 1 billion web requests each day, MessageLabs provides a range of information on global email security threats based on live data feeds from its control towers around the world.

The information relating to MessageLabs services contained in this report is based on data generated internally by MessageLabs unless otherwise indicated.

For more information on MessageLabs Intelligence and the analysis provided, please visit: www.messagelabs.com/intelligence

NB: All figures mentioned in this report were correct at the time of going to press.

MessageLabs is a leading provider of integrated messaging and web security services, with over 17,000 clients ranging from small business to the Fortune 500 located in more than 86 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.